GFI LanGuard™

Guía de instalación y configuración

GFI®

La información y el contenido de este documento se proporcionan sólo para fines informativos y "como están", sin garantía de ningún tipo, ya sea expresa o implícita, incluidas, sin limitarse a, las garantías implícitas de comercialización, idoneidad para un propósito particular y ausencia de infracción. GFI Software no se hace responsable por ningún daño, incluidos los daños indirectos de cualquier naturaleza que puedan deberse a la utilización de este documento. La información se ha obtenido de fuentes disponibles públicamente. A pesar de los esfuerzos razonables que se han hecho para asegurar la exactitud de los datos facilitados, GFI no afirma, promete ni garantiza la integridad, exactitud, actualidad o adecuación de la información, y no se responsabiliza por errores tipográficos, datos desactualizados o errores. GFI no ofrece ninguna garantía, expresa o implícita, y no asume ninguna responsabilidad civil o legal por la exactitud o la compleción de la información de este documento.

Si cree que existe algún error objetivo en este documento, póngase en contacto con nosotros y daremos tratamiento a sus dudas tan pronto como sea posible.

Todos los nombres de productos y empresas mencionados aquí pueden ser marcas comerciales de sus respectivos titulares.

GFI LanGuard es propiedad de GFI SOFTWARE Ltd. - 1999-2015 GFI Software Ltd. Reservados todos los derechos.

Versión del documento: 11.4

Última actualización (mes/día/año): 02/02/2015

Lista de tablas

Tabla 1: Términos y convenciones que se utilizan en este manual 4
Tabla 2: Componentes de GFI LanGuard 6
Tabla 3: Requisitos de hardware: GFI LanGuard Server 11
Tabla 4: Requisitos de hardware: agente de GFI LanGuard 11
Tabla 5: Requisitos de hardware: agente de retransmisión de GFI LanGuard 12
Tabla 6: Sistemas operativos compatibles 12
Tabla 7: Características admitidas por dispositivo, sistemas operativos y aplicaciones 13
Tabla 8: Back-end de base de datos compatibles 15
Tabla 9: Requisitos de software: componentes adicionales 15
Tabla 10: Puertos y protocolos 16
Tabla 11: Opciones de invalidación de importación 20
Tabla 12: Opciones de búsqueda 28
Tabla 13: Acciones del panel 32
Tabla 14: Información de software de una auditoría 34
Tabla 15: Vista según la información de los equipos 36
Tabla 16: Acciones del panel 39
Tabla 17: Acciones 43
Tabla 18: Problemas comunes de GFI LanGuard 47
Tabla 19: Opciones de recopilación de información 50

1 Introducción

GFI LanGuard es una solución de administración de revisiones y auditoría de redes que le permite administrar y mantener fácilmente la protección de terminales en dispositivos de su LAN. Actúa como un asesor de seguridad que ofrece asistencia para administración de revisiones, evaluación de vulnerabilidades y auditoría de redes para equipos con Windows®, Linux y MAC, así como para dispositivos móviles. GFI LanGuard logra la protección de LAN a través de lo siguiente:

- Identificación de puntos débiles de sistema y de red a través de una base de datos de comprobación de vulnerabilidades abarcadora. Esto incluye pruebas basadas en las directrices de evaluación de vulnerabilidades de OVAL y CVE, y en las 20 directrices de evaluación de vulnerabilidades principales del SANS
- Auditoría de todos los recursos de hardware y software de su red, lo que le permite crear un inventario de recursos detallado. Esto abarca incluso hasta la enumeración de aplicaciones instaladas y dispositivos conectados en su red
- Descarga automática e instalación remota de Service Pack y revisiones para los sistemas operativos Microsoft® Windows, Linux y MAC y productos de terceros
- Desinstalación automática de software no autorizado.

Temas de este capítulo:

1.1 Acerca de esta guía 4
1.2 Cómo funciona GFI LanGuard 5
1.3 Cómo funcionan los agentes de GFI LanGuard 5
1.4 Cómo funcionan los agentes de retransmisión de GFI LanGuard 6
1.5 Componentes de GFI LanGuard 6

1.1 Acerca de esta guía

El objetivo de esta Guía de instalación y configuración es ayudar a los administradores de sistemas a instalar y probar GFI LanGuard con un mínimo esfuerzo.

1.1.1 Términos y convenciones que se utilizan en este manual

Tabla 1: Términos y convenciones que se utilizan en este manual

Término	Descripción
	Información adicional y referencias esenciales para el funcionamiento de GFI LanGuard.
	Notificaciones y precauciones importantes sobre problemas comunes que pueden surgir.
>	Instrucciones de navegación paso a paso para acceder a una función concreta.
Texto en negrita	Elementos que se seleccionan, como nodos, opciones de menú o botones de comando.
Texto en cursiva	Parámetros y valores que debe reemplazar por los valores aplicables, como rutas de acceso y nombres de archivo personalizados.
`Código`	Indica los valores de texto que se escriben, como comandos y direcciones.

1.2 Cómo funciona GFI LanGuard

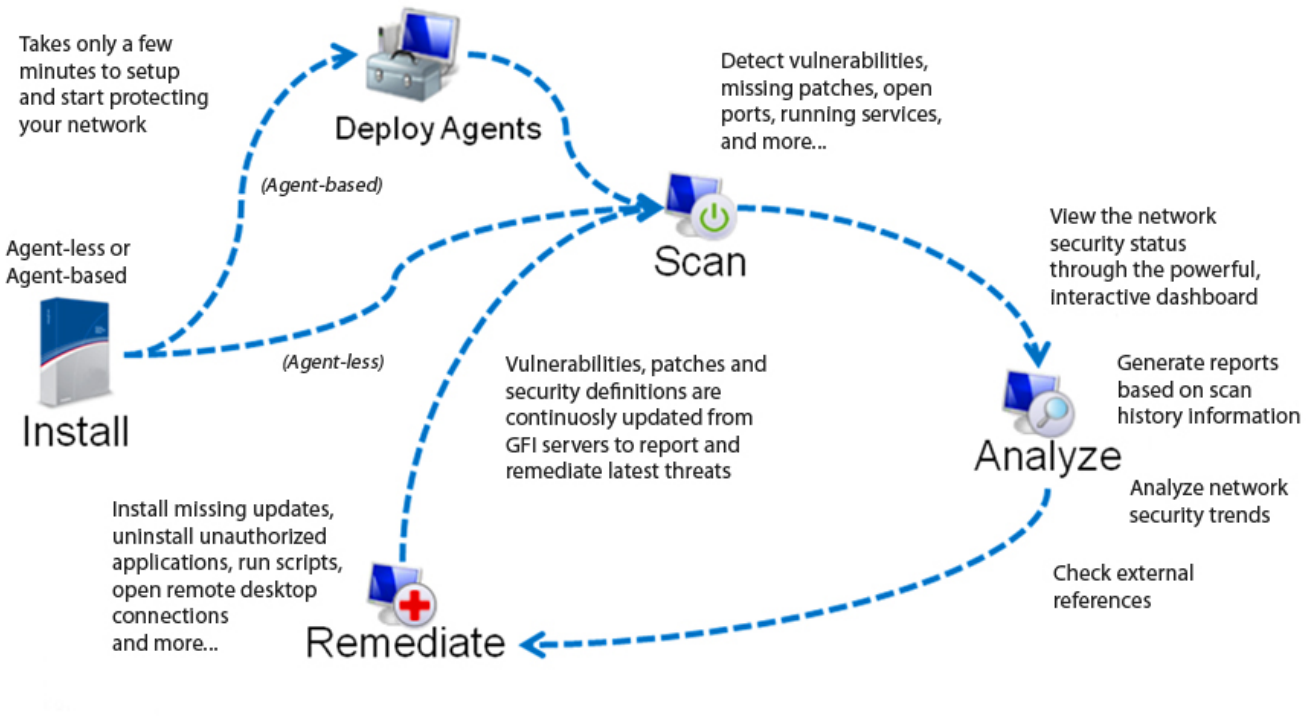

Takes only a few minutes to setup and start protecting your network
Deploy Agents
(Agent-based)
Agent-less or Agent-based
Install
(Agent-less)
Detect vulnerabilities, missing patches, open ports, running services, and more...
Scan
View the network security status through the powerful, interactive dashboard
Generate reports based on scan history information
Analyze
Analyze network security trends
Check external references
Vulnerabilities, patches and security definitions are continuosly updated from GFI servers to report and remediate latest threats
Install missing updates, uninstall unauthorized applications, run scripts, open remote desktop connections and more...
Remediate

Figura 1: Cómo funciona GFI LanGuard

Después de la instalación, GFI LanGuard funciona en dos etapas:

- En primer lugar, determina los equipos que están al alcance. También intenta recopilar conjuntos de información de los equipos de destino como parte de sus operaciones de Detección de redes, a través de un subconjunto de protocolos SMB, NETBIOS e ICMP. Entre los objetivos compatibles se incluyen el localhost, el IP, el nombre del equipo, la lista de equipos, el intervalo de IP, el dominio y grupo de trabajo completo o la unidad organizativa.
- En segundo lugar, una vez identificados los objetivos, GFI LanGuard realiza un examen en profundidad para enumerar toda la información relacionada con el equipo de destino. GFI LanGuard utiliza varias técnicas para acceder a esta información, la cual incluye verificaciones de propiedades de archivos y carpetas, verificaciones de registro, comandos de WMI y SMB, verificaciones de rastreo de puertos (TCP/UDP) y más.

1.3 Cómo funcionan los agentes de GFI LanGuard

GFI LanGuard se puede configurar para detectar e implementar agentes de forma automática en equipos nuevos. Los agentes minimizan la utilización de ancho de banda de la red. Esto se debe a que en el modo sin agente, el componente del servidor de GFI LanGuard realiza auditorías a través de la red, mientras que en el modo de agente, las auditorías se realizan utilizando los recursos del destino del examen y solo se transfiere un archivo XML de resultados a través de la red.

Los agentes envían datos aGFI LanGuard a través del puerto TCP 1070. Este puerto se abre de forma predeterminada al instalar GFI LanGuard. Los agentes no consumen recursos del equipo de destino del examen a menos que esté realizando un examen u operaciones de corrección. Si un agente no responde durante 60 días se desinstala de forma automática del equipo de destino.

Nota

De forma predeterminada, los agentes se desinstalan automáticamente al cabo de los 60 días. Para personalizar el periodo, seleccione la ficha **Configuration** y después **Agents Management**, y en el panel derecho haga clic en **Agents Settings**. Especifique el número de días en la ficha **General** del cuadro de diálogo **Agents Settings**.

Nota

Los agentes solo se pueden instalar en equipos con el sistema operativo Microsoft Windows y requieren aproximadamente 25 MB de memoria y 350 MB de espacio en disco duro.

1.4 Cómo funcionan los agentes de retransmisión de GFI LanGuard

GFI LanGuard le permite configurar cualquier equipo con un agente de GFI LanGuard instalado para que funcione como un servidor de GFI LanGuard. Estos agentes se denominan **Agentes de retransmisión**. Los agentes de retransmisión reducen la carga del componente del servidor de GFI LanGuard. Los equipos configurados como agentes de retransmisión descargan revisiones y definiciones directamente del servidor de GFI LanGuard y las reenvían a equipos clientes como si fueran componentes de servidores.

1.5 Componentes de GFI LanGuard

En esta sección se le brinda información acerca de los componentes que se instalan de forma predeterminada cuando realiza la instalación de GFI LanGuard. Una vez que instale el producto, puede gestionar las tareas de administración y corrección de revisiones desde la Consola de administración. La Consola de administración también se cita como el Componente del servidor deGFI LanGuard, como se describe en la tabla a continuación:

Tabla 2: Componentes de GFI LanGuard

Componente	Descripción
Servidor de GFI LanGuard	También denominado Consola de administración. Le permite administrar agentes, realizar exámenes, analizar resultados, corregir problemas de vulnerabilidad y generar informes.
GFI LanGuard Agents	Permite el procesamiento y la auditoría de datos en los equipos de destino; una vez finalizada una auditoría, el resultado se envía a GFI LanGuard.
GFI LanGuard Update System	Le permite establecer mediante configuración GFI LanGuard la descarga automática de actualizaciones publicadas por GFI para mejorar la funcionalidad. Para estas actualizaciones también incluye la búsqueda de actualizaciones más nuevas en el sitio web de GFI.
GFI LanGuard Attendant Service	El servicio de fondo que administra todas las operaciones programadas, incluidos los exámenes de seguridad de red, la implementación de revisiones y las operaciones de corrección.
GFI LanGuard Scanning Profiles Editor	Este editor le permite crear perfiles de detección nuevos y modificar los existentes.
GFI LanGuard Command Line Tools	Le permite iniciar exámenes de vulnerabilidad de la red y sesiones de implementación de revisiones, además de importar y exportar perfiles y vulnerabilidades sin cargar la consola de administración de GFI LanGuard.

2 Instalación de GFI LanGuard

Este capítulo le servirá como guía para seleccionar la solución de implementación que resulte más apropiada, cumpla con sus requisitos y le proporcione información acerca de cómo implementar con éxito un GFI LanGuard totalmente funcional.

Temas de este capítulo:

2.1 Escenarios de implementación 7
2.2 Requisitos del sistema 11
2.3 Actualización de versiones anteriores 17
2.4 Acciones posteriores a la instalación 19

2.1 Escenarios de implementación

GFI LanGuard se puede instalar en cualquier equipo que cumpla con los requisitos de sistema mínimos. Utilice la información de esta sección para determinar si desea controlar un conjunto "sin agente" y "basado en agente", o una mezcla de ambos, según lo siguiente:

- Número de equipos y dispositivos que desea controlar
- Carga de tráfico de su red durante el tiempo de operación normal.

En las secciones siguientes se le proporciona información acerca de diferentes escenarios de implementación admitidos por GFI LanGuard:

- Implementación de GFI LanGuard en el modo mixto
- Implementación de GFI LanGuard mediante agentes de retransmisión
- Implementación de GFI LanGuard en el modo sin agente

2.1.1 Implementación de GFI LanGuard en el modo mixto

GFI LanGuard se puede configurar para implementar agentes de forma automática en equipos recién detectados o seleccionados manualmente. Los agentes permiten que el procesamiento y la auditoría de datos se realicen en equipos de destino; una vez que una auditoría finaliza, el resultado se transfiere a GFI LanGuard a través de un archivo XML. Exámenes basados en agentes:

- Tienen un mejor rendimiento porque la carga se distribuye en equipos cliente.
- Pueden funcionar en entornos de ancho de banda reducido porque la comunicación entre el servidor y los agentes es reducida.
- Son adecuados para portátiles. Los equipos se examinarán aun cuando no estén conectados a la red de la empresa.
- Son más precisos que los exámenes manuales; los agentes pueden acceder a más información en el localhost.

En la siguiente captura de pantalla se muestra cómo se puede implementar GFI LanGuard utilizando agentes de una red de área local (LAN):

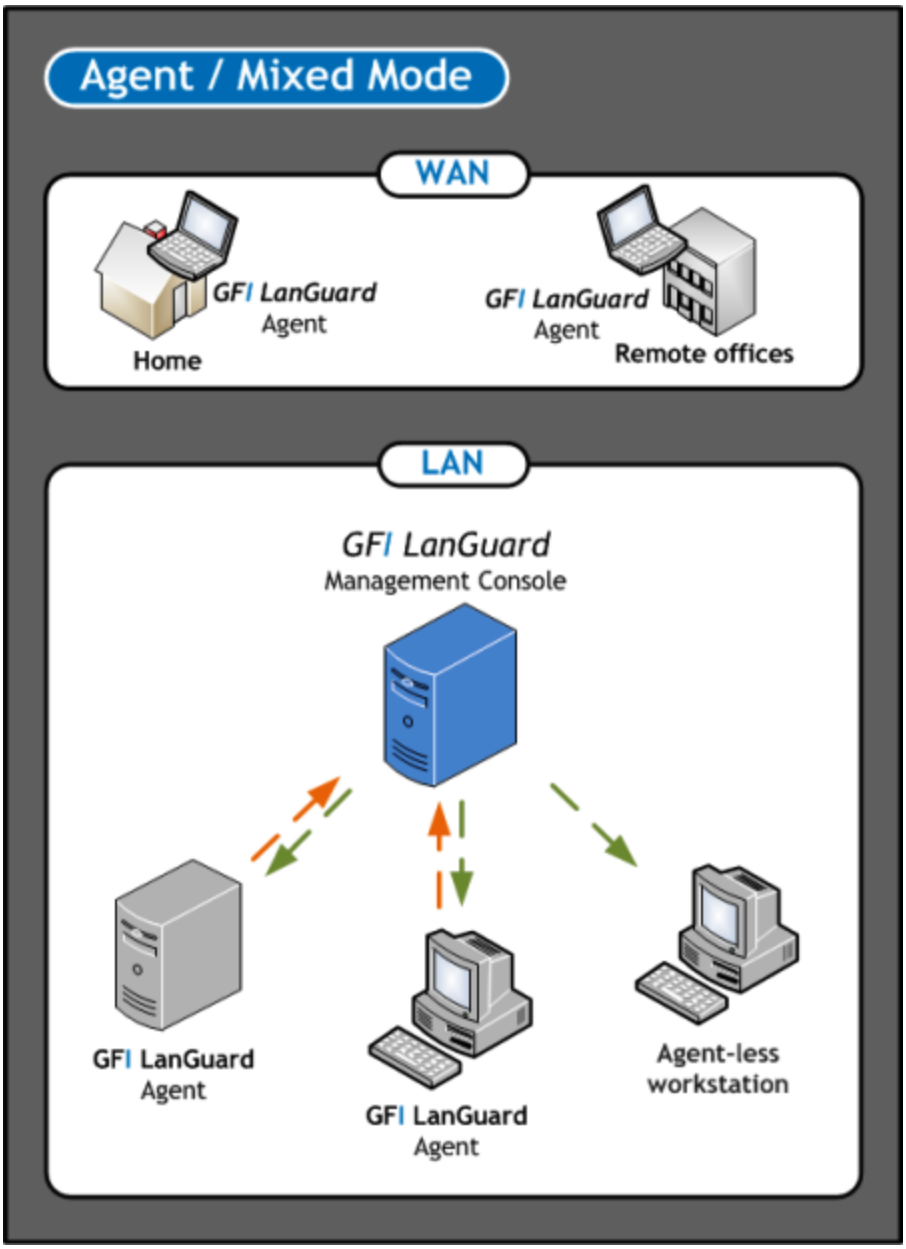


Figura 2: Modo de agente o mixto

2.1.2 Implementación de GFI LanGuard mediante agentes de retransmisión

Los agentes de retransmisión se utilizan para reducir la carga del servidor de GFI LanGuard. Los equipos configurados como agentes de retransmisión descargarán revisiones y definiciones directamente del servidor de GFI LanGuard y las reenviarán a equipos clientes. Las ventajas principales de utilizar agentes de retransmisión son las siguientes:

- Ahorro de ancho de banda de red en redes locales o distribuidas geográficamente. Si se configura un agente de retransmisión en cada sitio, una revisión solo se descarga una vez y se distribuye a los clientes
- La carga se quita del componente del servidor de GFI LanGuard y se distribuye entre los agentes de retransmisión
- Debido a que los equipos se administran desde varios agentes de retransmisión, aumenta el número de dispositivos que se pueden proteger de forma simultánea.

En una red, los equipos se pueden agrupar y cada grupo se puede asignar a un agente de retransmisión, como se muestra a continuación.

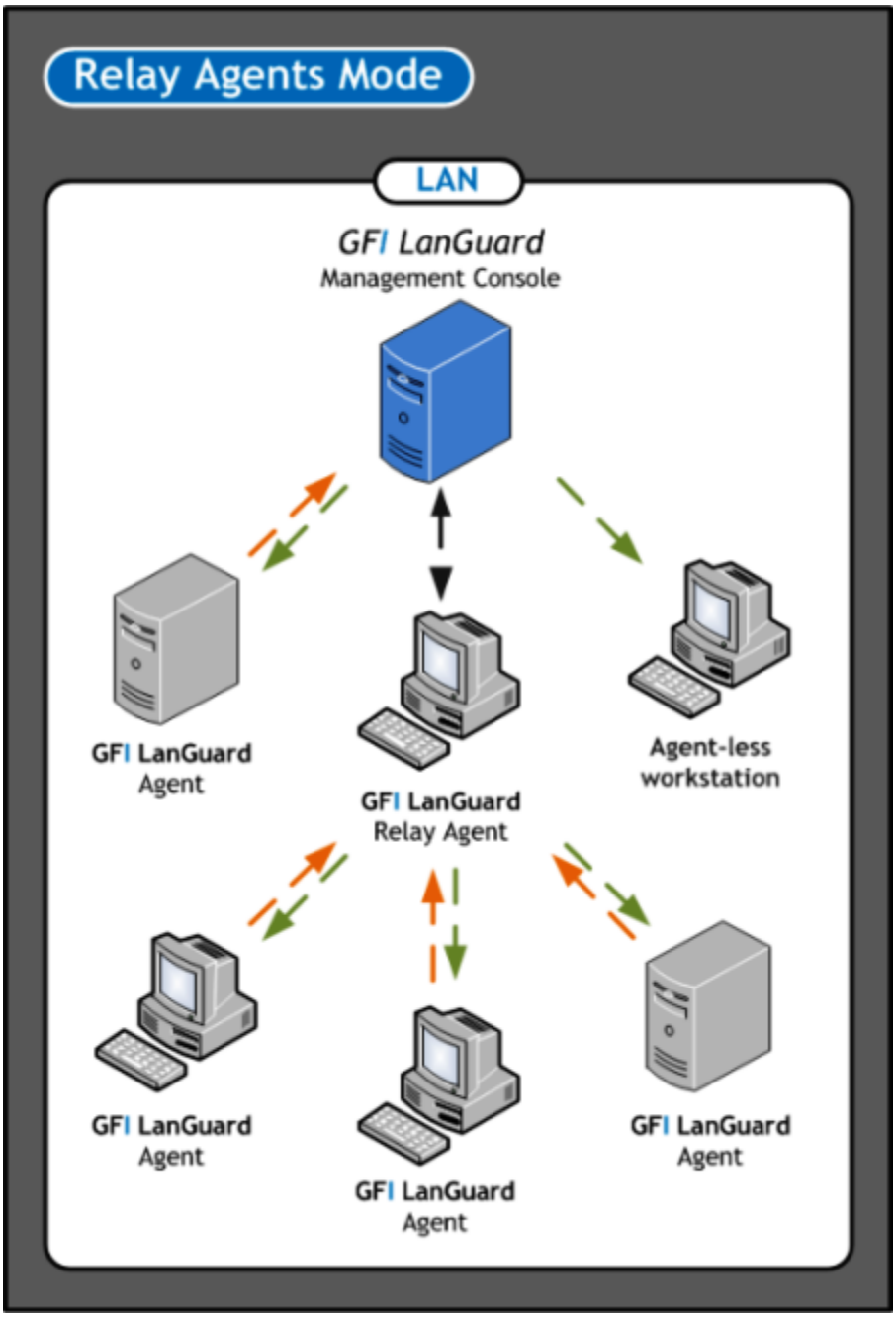


Figura 3: Modo de agente de retransmisión

> **Nota**
>
> Para obtener más información, consulte **Configuración de agentes de retransmisión** en la **Guía del administrador**.

2.1.3 Implementación de GFI LanGuard en el modo sin agente

La auditoría sin agente se inicia desde la consola de administración de GFI LanGuard. GFI LanGuard crea una sesión remota con los destinos de examen especificados y los audita en la red. Al

completarse el proceso, se importan los resultados a la base de datos de resultados y se cierra la sesión remota.

Puede auditar equipos de forma individual, un rango de equipos específicos y un dominio o grupo de trabajo completos.

> **Nota**
>
> Los exámenes en el modo sin agente utilizan los recursos del equipo en el cual GFI LanGuard está instalado y emplean más ancho de banda de red debido a que la auditoría se realiza de forma remota. Cuando se dispone de una red grande de destinos de examen, este modo puede reducir drásticamente el rendimiento de GFI LanGuard' y afectar la velocidad de la red. En redes más grandes, implemente agentes convencionales o de retransmisión para equilibrar la carga de forma adecuada.

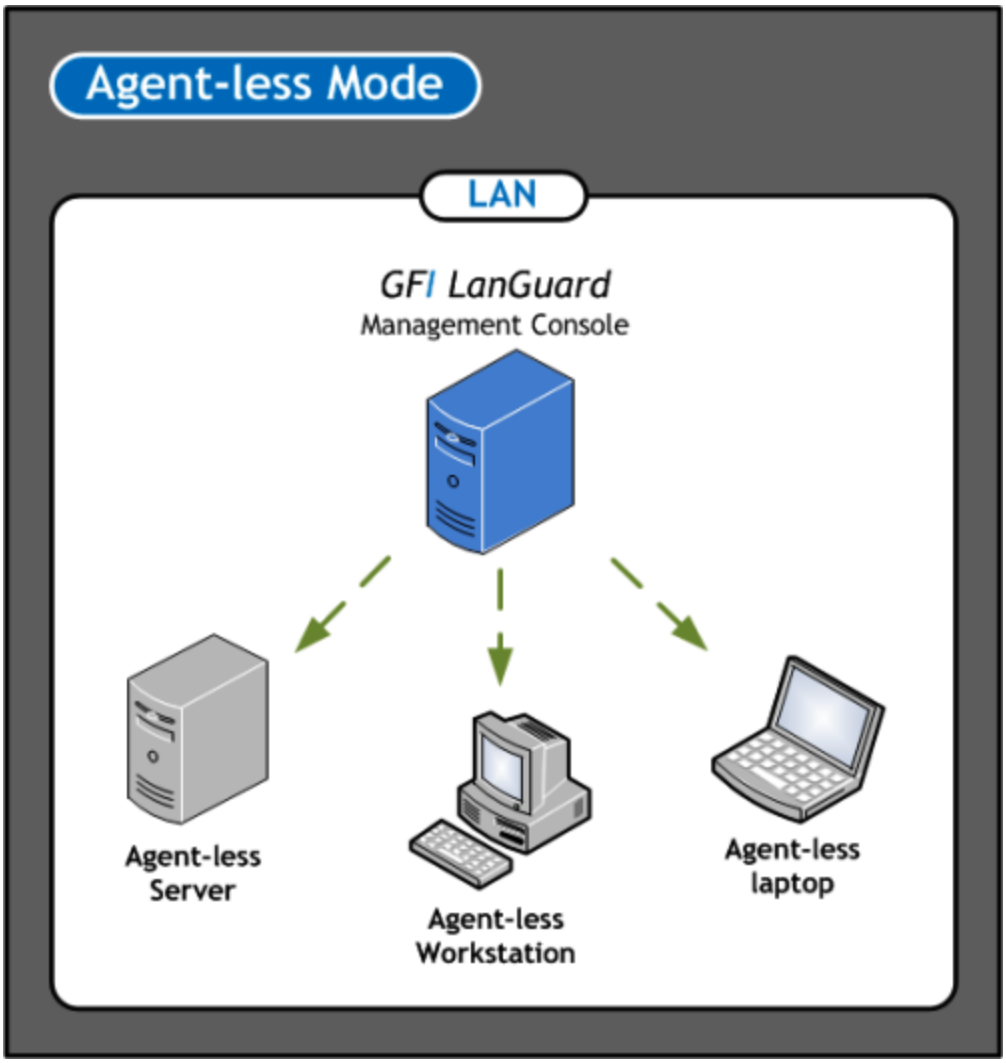


Figura 4: Modo sin agente

2.2 Requisitos del sistema

Los equipos en los que se ejecuten un GFI LanGuard servidor, un agente convencional y un agente de retransmisión deben cumplir con los requisitos de sistema descritos a continuación por razones de rendimiento.

> **Nota**
>
> Si busca una solución de administración de revisiones para 2.000 o más equipos, le recomendamos contactarnos para obtener cotizaciones y sugerencias relacionadas con el procedimiento de implementación y administración adecuado para dicha solución.

Consulte las secciones siguientes para obtener información sobre:

- Requisitos de hardware
- Requisitos de software
- Puertos y protocolos de cortafuegos
- Permisos de puertas de enlace
- Aplicaciones antivirus y antispyware compatibles

2.2.1 Requisitos de hardware

Asegúrese de que se cumplan los requisitos de hardware siguientes en equipos en los que se ejecute cualquiera de los componentes que se proporcionan a continuación:

- Servidor GFI LanGuard
- Agente convencionalGFI LanGuard
- Agente de retransmisiónGFI LanGuard

GFI LanGuard Servidor

El servidor de GFI LanGuard que aloje los equipos debe cumplir con los siguientes requisitos de hardware:

Tabla 3: Requisitos de hardware: GFI LanGuard Server

Componente	1 a 100 equipos	100 a 500 equipos	500 a 3.000 equipos
Procesador	De dos núcleos y 2 GHz	De dos núcleos y 2,8 GHz	De cuatro núcleos y 3 GHz
Almacenamiento físico	5 GB	10 GB	20 GB
RAM	2 GB	4 GB	8 GB
Ancho de banda de red	1544 kbps	1544 kbps	1544 kbps

Agente GFI LanGuard

Los equipos en los que se ejecute un agente de GFI LanGuard deben cumplir con los siguientes requisitos de hardware:

Tabla 4: Requisitos de hardware: agente de GFI LanGuard

Componente	Requisito
Procesador	1 GHz
Almacenamiento físico	1,5 GB

Componente	Requisito
RAM	25 MB
Ancho de banda de red	1544 kbps

Agente de retransmisión GFI LanGuard

Un equipo se podrá configurar como agente de retransmisión cuando:

- El equipo debe estar en línea y tener un buen tiempo de actividad (un agente de retransmisión fuera de línea anula las capacidades de sus clientes)
- Tenga un acceso rápido a equipos conectados a él
- Tenga el espacio en disco necesario para permitir el almacenamiento en caché.

Los equipos configurados como agentes de retransmisión deben cumplir con los siguientes requisitos de hardware:

Tabla 5: Requisitos de hardware: agente de retransmisión de GFI LanGuard

Componente	1 a 100 clientes	100 a 500 clientes	500 a 1000 clientes
Procesador	De dos núcleos y 2 GHz	De dos núcleos y 2 GHz	De dos núcleos y 2,8 GHz
Almacenamiento físico	5 GB	10 GB	10 GB
RAM	2 GB	2 GB	4 GB
Ancho de banda de red	100 Mbps	100 Mbps	1 Gbps

2.2.2 Requisitos de software

Los componentes de GFI LanGuard se pueden instalar en cualquier equipo que cumpla con los requisitos de software enumerados en esta sección. Para obtener más información, consulte:

- Sistemas operativos compatibles
- Características por dispositivo, sistemas operativos y aplicaciones compatibles
- Bases de datos compatibles
- Componentes en los equipos de destino
- Otros componentes de software

sistemas operativos compatibles (32 y 64 bits)

En la siguiente tabla se enumeran sistemas operativos en los que se pueden instalar un servidor, agente convencional o agente de retransmisión de GFI LanGuard:

Tabla 6: Sistemas operativos compatibles

Operating System	GFI LanGuard	Agente GFI LanGuard	Agente de retransmisión GFI LanGuard
Windows ® Server 2012 (incluso R2)	✓	✓	✓
Windows® Server 2008 (incluido R2) Standard o Enterprise	✓	✓	✓
Windows® Server 2003 Standard o Enterprise	✓	✓	✓
Windows® 8 Professional/Enterprise (incluso Windows®8.1)	✓	✓	✓
Windows® 7 Professional, Enterprise o Ultimate	✓	✓	✓
Windows® Vista Business, Enterprise o Ultimate	✓	✓	✓

Operating System	GFI LanGuard	Agente GFI LanGuard	Agente de retransmisión GFI LanGuard
Windows® XP Professional (SP2 o superior)	✓	✓	✓
Windows® Small Business Server 2011	✓	✓	✓
Windows® Small Business Server 2008 Standard	✓	✓	✓
Windows® Small Business Server 2003 (SP1)	✓	✓	✓
Windows® 2000 Professional, Server o Advanced » SP4 » Internet Explorer 6 SP1 o superior » Windows Installer 3.1 o superior	✗	✓	✓

Características por dispositivo, sistemas operativos y aplicaciones compatibles.

En la siguiente tabla se mencionan características, sistemas operativos y aplicaciones compatibles:

Tabla 7: Características admitidas por dispositivo, sistemas operativos y aplicaciones

	Identificación de dispositivos y examen de puertos	Evaluación de vulnerabilidades	Administración de revisiones	Software Audit	Hardware Audit
Windows ® Server 2012 (incluso R2)	✓	✓	✓	✓	✓
Windows® Server 2008 (incluido R2) Standard o Enterprise	✓	✓	✓	✓	✓
Windows® Server 2003 Standard o Enterprise	✓	✓	✓	✓	✓
Windows® Small Business Server 2011	✓	✓	✓	✓	✓
Windows® Small Business Server 2008 Standard	✓	✓	✓	✓	✓
Windows® Small Business Server 2003 (SP1)	✓	✓	✓	✓	✓
Windows® Server 2000	✓	✓	✓	✓	✓
Versiones de cliente de Windows					
Windows® 8 Professional/Enterprise (incluso Windows®8.1)	✓	✓	✓	✓	✓
Windows® 7 Professional, Enterprise o Ultimate	✓	✓	✓	✓	✓
Windows® Vista Business, Enterprise o Ultimate	✓	✓	✓	✓	✓
Windows® XP Professional (SP2 o superior)	✓	✓	✓	✓	✓
Windows® 2000 Professional (SP4)	✓	✓	✓	✓	✓
Aplicaciones de terceros de Windows					
Microsoft® Office	✗	✓	✓	✗	✗

	Identificación de dispositivos y examen de puertos	Evaluación de vulnerabilidades	Administración de revisiones	Software Audit	Hardware Audit
Microsoft® Exchange	✗	✓	✓	✗	✗
Microsoft® SQL Server	✗	✓	✓	✗	✗
Microsoft® Visual Studio	✗	✓	✓	✗	✗
Otras aplicaciones de Microsoft® (haga clic para obtener la lista completa)	✗	✓	✓	✗	✗
Java Runtime Environment	✗	✓	✓	✗	✗
Adobe Flash Player	✗	✓	✓	✗	✗
Adobe Reader	✗	✓	✓	✗	✗
Adobe AIR	✗	✓	✓	✗	✗
Adobe Shockwave Player	✗	✓	✓	✗	✗
Mozilla Firefox	✗	✓	✓	✗	✗
Apple Safari	✗	✓	✓	✗	✗
Apple QuickTime	✗	✓	✓	✗	✗
Apple iTunes	✗	✓	✓	✗	✗
Explorador Opera	✗	✓	✓	✗	✗
Otros proveedores (Haga clic aquí para obtener la lista completa)	✗	✓	✓	✗	✗
Distribuciones de Linux					
Mac OS X 10.5 y superiores	✓	✓	✓	✓	✓
Red Hat Enterprise Linux 5 y superiores	✓	✓	✓	✓	✓
CentOS 5 y superiores	✓	✓	✓	✓	✓
Ubuntu 10.04 y superiores	✓	✓	✓	✓	✓
Debian 6 y superiores	✓	✓	✓	✓	✓
SUSE Linux Enterprise 11.2 y superiores	✓	✓	✓	✓	✓
OpeSUSE 11 y superiores	✓	✓	✓	✓	✓
Otras distribuciones	✓	✓	✗	✓	✓
Equipos virtuales (con sistemas operativos compatibles)					
Vmware	✓	✓	✓	✓	✓

	Identificación de dispositivos y examen de puertos	Evaluación de vulnerabilidades	Administración de revisiones	Software Audit	Hardware Audit
Microsoft® Hyper-V	✓	✓	✓	✓	✓
Microsoft® Virtual PC	✓	✓	✓	✓	✓
Oracle Virtual Box	✓	✓	✓	✓	✓
Citrix Xen	✓	✓	✓	✓	✓
Paralelos	✓	✓	✓	✓	✓
Network Devices					
Cisco (Haga clic para obtener la lista completa)	✓	✓	✗	✗	✗
HP (Haga clic para obtener la lista completa)	✓	✓	✗	✗	✗
Otros proveedores	✓		✗	✗	✗
Dispositivos móviles:					
Google Android	✓	✓	✗	✗	✗
Apple iOS	✓	✓	✗	✗	✗
Windows Phone	✓	✓	✗	✗	✗

Bases de datos compatibles

GFI LanGuard utiliza una base de datos para almacenar información de auditorías de seguridad de red y operaciones de corrección. El back-end de base de datos puede ser cualquiera de los siguientes:

Tabla 8: Back-end de base de datos compatibles

Base de datos	Utilización recomendada
Microsoft ® Access	Se recomienda únicamente durante la evaluación y para un total de hasta 5 equipos.
MSDE/SQL Server Express® edition	Se recomienda para redes de hasta 500 equipos.
SQL Server® 2000 o posterior	Se recomienda para redes más grandes de hasta 500 equipos o más.

Componentes en los equipos de destino

En la siguiente tabla se le proporciona información acerca de componentes que se deben instalar o habilitar en equipos que se examinarán de forma remota a través de GFI LanGuard:

Tabla 9: Requisitos de software: componentes adicionales

Componente	Descripción
Secure Shell (SSH)	Se requiere para destinos de examen basados en UNIX, Linux y Max OS. Se incluye comúnmente como parte de todas las distribuciones de Unix o Linux.
Windows Management Instrumentation (WMI)	Se requiere para destinos de examen basados en Windows. Se incluye en todos los sistemas operativos Windows 2000 o posteriores.
Uso compartido de archivos e impresoras	Se requiere para enumerar y recopilar información sobre destinos de examen.
Registro remoto	Se requiere para que GFI LanGuard ejecute un servicio temporal para el examen de un destino remoto.

Componentes de servidor de GFI LanGuard adicionales

El siguiente componente adicional se requiere en el equipo en el que se instale el componente de servidor de GFI LanGuard:

- Microsoft .NET® Framework 3.5.

2.2.3 Puertos y protocolos de cortafuegos

En esta sección se le proporciona información acerca de la configuración de puertos y protocolos de cortafuegos necesaria para:

- GFI LanGuardAgentes de servidores y de retransmisión
- GFI LanGuard Equipos con y sin agentes

Agentes de GFI LanGuard y de retransmisión

Configure su cortafuegos de modo que permita conexiones **entrantes** en el puerto TCP **1070** en equipos en los que se ejecuten:

- GFI LanGuard
- Agentes de retransmisión

Este puerto se utiliza de forma automática cuando se instala GFI LanGuard y manipula toda comunicación entrante entre el componente del servidor y los equipos controlados. Si GFI LanGuard detecta que el puerto 1070 ya se encuentra en uso a través de otra aplicación, busca de forma automática un puerto disponible dentro del rango del **1070 al 1170**.

Para configurar de forma manual el puerto de comunicaciones:

1. Inicie GFI LanGuard.

2. Haga clic en la ficha **Configuration** y en **Manage Agents**.

3. En el panel derecho, haga clic en **Agents Settings**.

4. Desde el cuadro de diálogo **Agents Settings**, especifique el puerto de comunicaciones en el cuadro de texto **TCP port**.

5. Haga clic en **OK**.

GFI LanGuard Equipos con y sin agentes

GFI LanGuard se comunica con equipos administrados (con y sin agentes) utilizando los puertos y protocolos siguientes. En los equipos administrados, el cortafuegos se debe configurar de modo que permita solicitudes **entrantes** en los puertos:

Tabla 10: Puertos y protocolos

Puertos TCP	Protocolo	Descripción
22	SSH	Auditoría de sistemas Linux.
135	DCOM	Puerto asignado de forma dinámica.
137	NetBIOS	Detección de equipos y uso compartido de recursos.
138	NetBIOS	Detección de equipos y uso compartido de recursos.
139	NetBIOS	Detección de equipos y uso compartido de recursos.
161	SNMP	Detección de equipos.

Puertos TCP	Protocolo	Descripción
445	SMB	Se utiliza durante: » Auditoría de equipos » Administración de agentes » Implementación de revisiones.

2.2.4 Permisos de puertas de enlace

Para descargar actualizaciones de definiciones de seguridad, GFI LanGuard se conecta a servidores de actualización de GFI, de Microsoft y de proveedores independientes mediante HTTP. Asegúrese de que la configuración del cortafuegos del equipo en el que GFI LanGuard está instalado permita las conexiones a:

- *software.gfi.com/lnsupdate/
- *.download.microsoft.com
- *.windowsupdate.com
- *.update.microsoft.com
- Todos los servidores de actualización de proveedores independientes admitidos por GFI LanGuard.

Nota

Para obtener más información, consulte:

- Aplicaciones compatibles de proveedores independientes:
  - http://go.gfi.com/?pageid=LAN_PatchMng
- Boletines de aplicación compatibles:
  - http://go.gfi.com/?pageid=3p_fullreport
- Aplicaciones de Microsoft compatibles:
  - http://go.gfi.com/?pageid=ms_app_fullreport
- Boletín de Microsoft compatible:
  - http://go.gfi.com/?pageid=ms_fullreport

2.2.5 Aplicaciones antivirus y antispyware compatibles

GFI LanGuard detecta archivos de definición obsoletos para varias aplicaciones de software antivirus y antispyware. Para obtener una lista completa de aplicaciones de software antivirus y antispyware compatibles, consulte lo siguiente: http://go.gfi.com/?pageid=security_app_fullreport

2.3 Actualización de versiones anteriores

GFI LanGuard conserva toda la información de configuración y resultados de cualquier versión anterior de GFI LanGuard. Esto le permite:

- Instalar GFI LanGuard sin desinstalar la versión anterior.
- Importar la configuración en GFI LanGuard desde otras instalaciones del programa.

» Implementar agentes en los mismos equipos en los que cuenta con una versión anterior de GFI LanGuard instalada.

Nota

No se pueden realizar actualizaciones de software de versiones de GFI LanGuard anteriores a la 9.

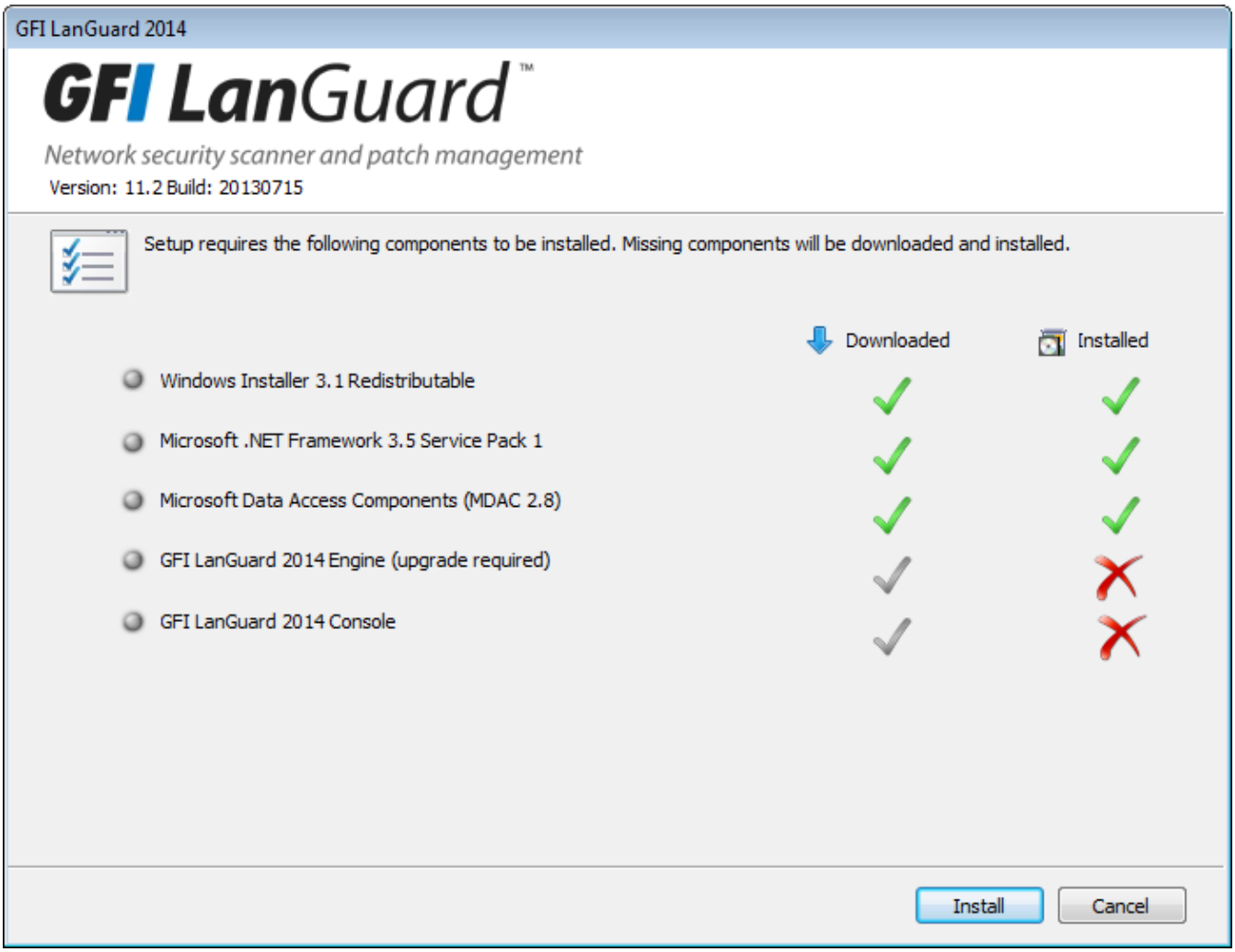
Nota

Las claves de licencia de versiones anteriores de GFI LanGuard no son compatibles y se deben actualizar para ejecutar GFI LanGuard.

Para realizar una actualización a una versión más nueva:

1. Inicie sesión utilizando credenciales de administrador en el equipo en el que desee instalar GFI LanGuard.

2. Inicie la instalación de GFI LanGuard.


GFI LanGuard 2014
GFI LanGuard
Network security scanner and patch management
Version: 11.2 Build: 20130715
Setup requires the following components to be installed. Missing components will be downloaded and installed.
Downloaded
Installed
Windows Installer 3.1 Redistributable
Microsoft .NET Framework 3.5 Service Pack 1
Microsoft Data Access Components (MDAC 2.8)
GFI LanGuard 2014 Engine (upgrade required)
GFI LanGuard 2014 Console
Install
Cancel

Captura de pantalla 1: Cuadro de diálogo de comprobación de requisitos previos

3. En el cuadro de diálogo de comprobación de requisitos previos se muestra información general del estado de los componentes que GFI LanGuard requiere para funcionar. Haga clic en **Install** para iniciar la instalación.

4. Siga las instrucciones en pantalla para completar la actualización.

5. Una vez que GFI LanGuard está instalado, detecta la instalación anterior e inicia de forma automática el **Import and Export Configurations Wizard**. Esto le permite exportar varias configuraciones de la versión anterior e importarlas a la nueva.

6. Seleccione las configuraciones que se importarán y haga clic en **Next** para finalizar el proceso de importación.

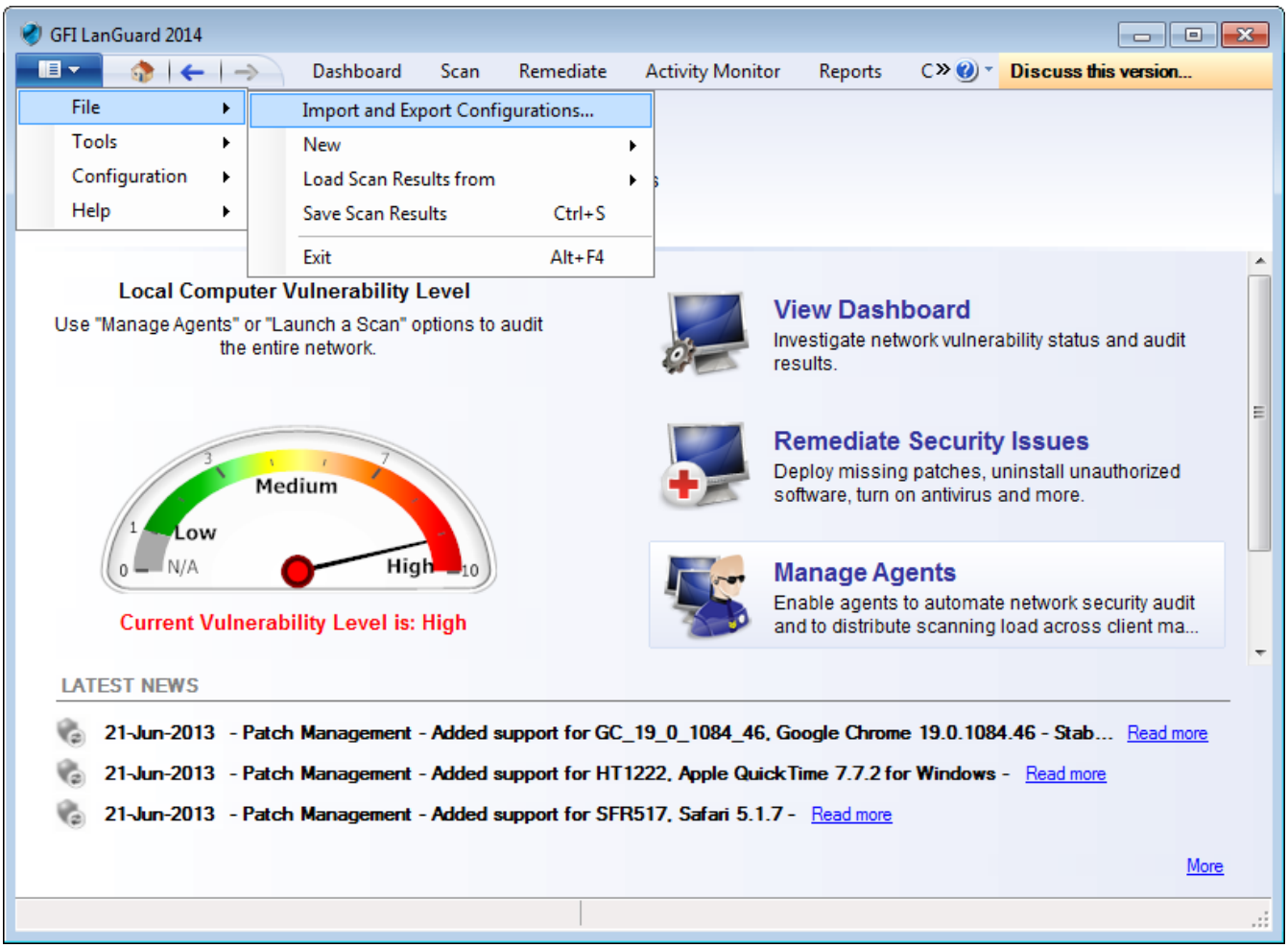
2.4 Acciones posteriores a la instalación

GFI LanGuard se puede instalar en un equipo con una versión anterior de GFI LanGuard sin necesidad de desinstalarla. Esto le permite conservar parámetros de configuración y reutilizarlos en la versión nueva.

Para importar la configuración de la versión anterior:

1. Inicie la consola de administración de GFI LanGuard desde **Inicio > Programas > GFI LanGuard 2015> GFI LanGuard 2015**.

2. En **GFI LanGuard**, haga clic en el botón **File y después en Import and Export Configurations…** para iniciar el **Import and Export Configurations wizard**.


GFI LanGuard 2014
Dashboard
Scan
Remediate
Activity Monitor
Reports
Discuss this version...
File
Tools
Configuration
Help
Import and Export Configurations...
New
Load Scan Results from
Save Scan Results Ctrl+S
Exit Alt+F4
Local Computer Vulnerability Level
Use "Manage Agents" or "Launch a Scan" options to audit the entire network.
Medium
Low
High
N/A
Current Vulnerability Level is: High
View Dashboard
Investigate network vulnerability status and audit results.
Remediate Security Issues
Deploy missing patches, uninstall unauthorized software, turn on antivirus and more.
Manage Agents
Enable agents to automate network security audit and to distribute scanning load across client ma...
LATEST NEWS
21-Jun-2013 - Patch Management - Added support for GC_19_0_1084_46, Google Chrome 19.0.1084.46 - Stab... Read more
21-Jun-2013 - Patch Management - Added support for HT1222, Apple QuickTime 7.7.2 for Windows - Read more
21-Jun-2013 - Patch Management - Added support for SFR517, Safari 5.1.7 - Read more
More

Captura de pantalla 2: Configuraciones de importación y exportación

3. Seleccione **Import the configuration from another instance** y haga clic en **Next**.

4. Haga clic en **Browse** para seleccionar la carpeta de instalación de GFI LanGuard. La ubicación predeterminada es:

- **Equipos de 64 bits (x64):** `<Disco local>\Program Files (x86)\GFI\ LanGuard <Versión>`
- **Equipos de 32 bits (x86):** `<Disco local>\Program Files\GFI\ LanGuard <Versión>`

5. Haga clic en **Next**.

6. Seleccione la configuración que se importará y haga clic en **Next**.

7. Durante la importación, GFI LanGuard le preguntará si desea invalidar o conservar su configuración existente. Seleccione:

Tabla 11: Opciones de invalidación de importación

Opción	Descripción
Sí	Invalidar la configuración actual a través de la configuración importada.
No	Conservar la configuración actual e ignorar la configuración importada.
Auto Rename	Cambiar el nombre de la configuración importada y mantener la configuración actual.

8. Haga clic en **OK** cuando haya finalizado.

3 Prueba de la instalación

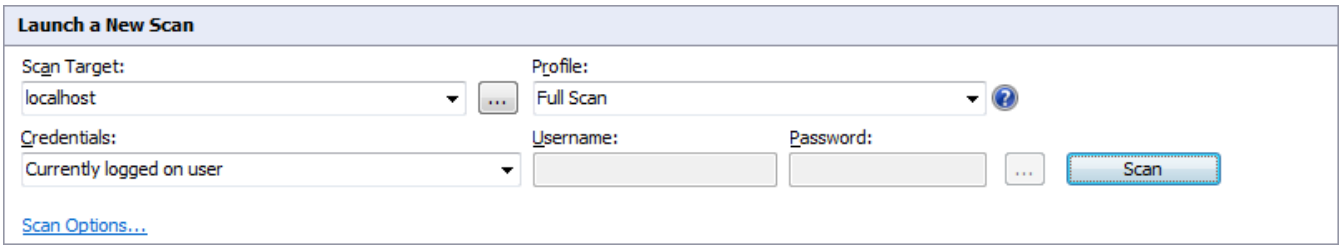
Una vez que GFI LanGuard esté instalado, pruebe la instalación ejecutando un examen local para asegurarse de que esté correctamente instalado.

1. Inicie GFI LanGuard.

GFI LanGuard 2014
Dashboard
Scan
Remediate
Activity Monitor
Reports
Discuss this version...
Welcome to GFI LanGuard 2014
GFI LanGuard 2014 is ready to audit your network for vulnerabilities
Medium
Low
N/A
High
Current Vulnerability Level is: High
Remediate Security Issues
Deploy missing patches, uninstall unauthorized software, turn on antivirus and more.
Manage Agents
Enable agents to automate network security audit and to distribute scanning load across client ma...
Launch a Scan
Manually set-up and trigger an agentless network security audit.
LATEST NEWS
21-Jun-2013 - Patch Management - Added support for GC_19_0_1084_46, Google Chrome 19.0.1084.46 - Stab... Read more
21-Jun-2013 - Patch Management - Added support for HT1222, Apple QuickTime 7.7.2 for Windows - Read more
21-Jun-2013 - Patch Management - Added support for SFR517, Safari 5.1.7 - Read more
More

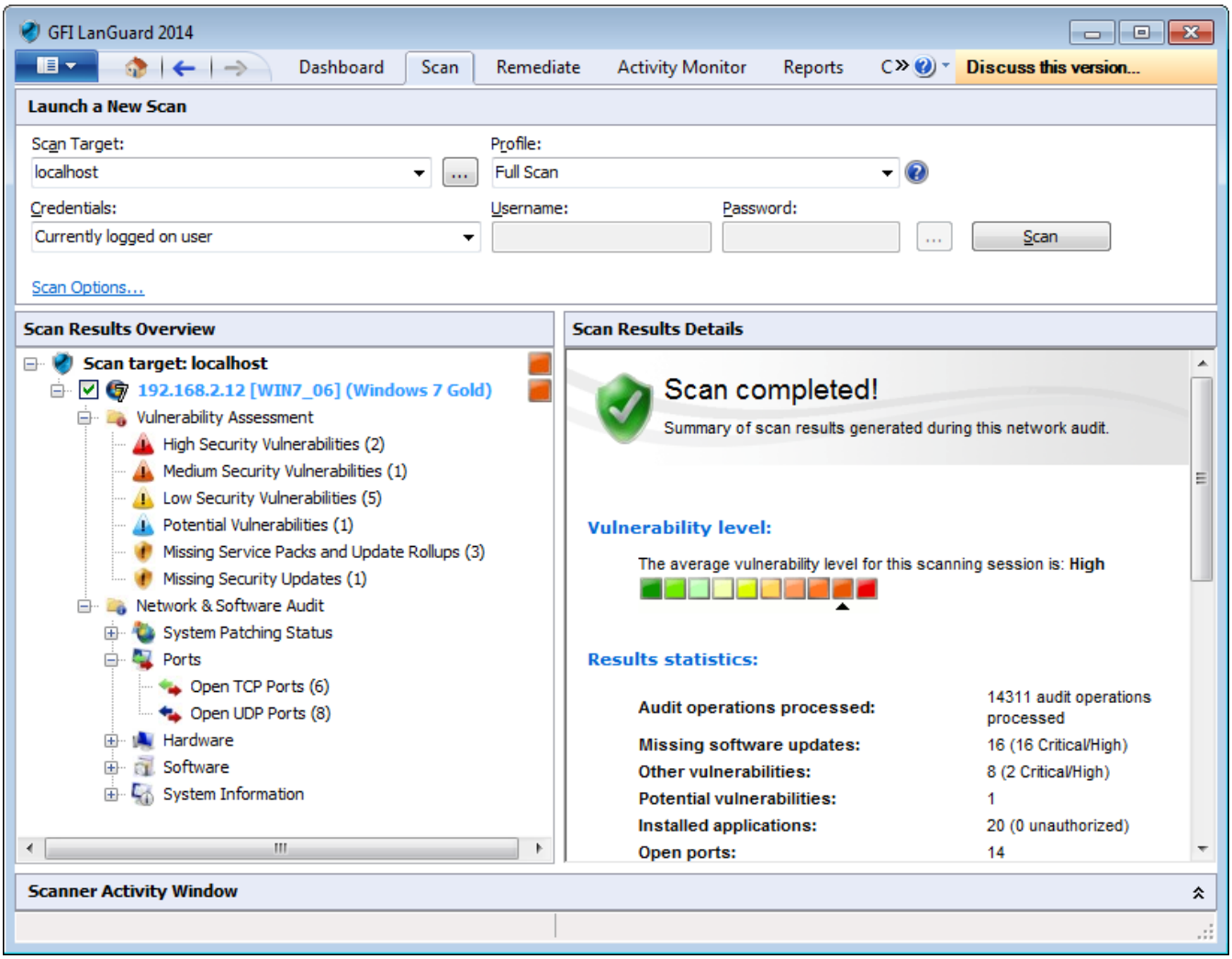
Captura de pantalla 3: Inicio de un examen

2. En la página de inicio de GFI LanGuard, haga clic en **Launch a Scan**.



Captura de pantalla 4: Propiedades de Launch a scan

3. En el menú desplegable de **Scan Target**, seleccione **localhost**.
4. En el menú desplegable de **Profile**, seleccione **Full Scan**.
5. Haga clic en **Scan** para iniciar el examen en el equipo local.
6. El progreso del examen se muestra en la ficha **Scan**.



Captura de pantalla 5: Resumen de resultados de examen

7. Una vez completado el proceso, en la sección **Progress** aparecerá información general del resultado del examen.

8. Utilice las secciones **Scan Results Details** y **Scan Results Overview** para analizar el resultado del examen.

4 El panel de GFI LanGuard

La sección **Dashboard** le proporciona información exhaustiva sobre seguridad según datos adquiridos durante auditorías. Entre otras posibilidades, el panel le permite determinar el nivel de vulnerabilidad actual de la red, los equipos más vulnerables y el número de equipos de la base de datos.

Temas de este capítulo:

4.1 Obtención de resultados a partir del panel 23
4.2 Utilización del panel 23
4.3 Utilización del árbol de equipos 24
4.4 Utilización de atributos 29
4.5 Acciones del panel 32
4.6 Exportación de la lista de problemas 32
4.7 Vistas del panel 33

4.1 Obtención de resultados a partir del panel

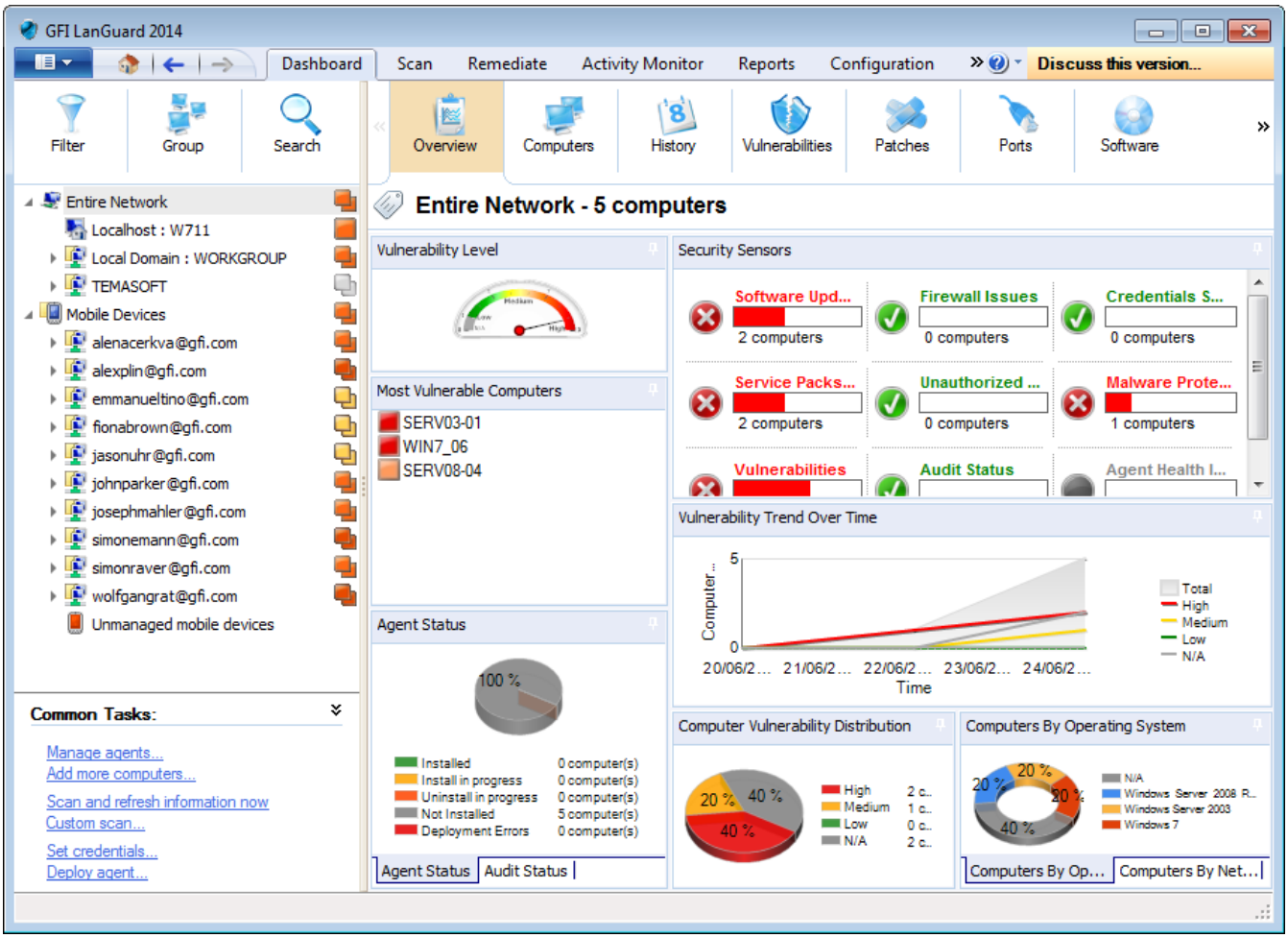
El panel es una característica importante de GFI LanGuard. Como elemento central de la aplicación, le permite realizar todas las tareas comunes que admite GFI LanGuard, incluidas las siguientes:

- Supervisión de todos los equipos administrados por GFI LanGuard
- Administración de destinos de examen. Adición, edición o eliminación de equipos, dominios y grupos de trabajo
- Implementación de agentes en destinos de examen y configuración de parámetros de agentes
- Configuración de credenciales de equipos
- Configuración de opciones de corrección automática
- Configuración de la detección de redes recurrentes en los dominios, los grupos de trabajo o las UO
- Desencadenamiento de exámenes de seguridad o actualización de información de exámenes
- Análisis del estado de seguridad de los equipos y de detalles de auditoría
- Cambio a ubicaciones relevantes haciendo clic en sensores y gráficos de seguridad.

4.2 Utilización del panel

En esta sección se proporciona información necesaria acerca de cómo utilizar el panel de GFI LanGuard. Para que aparezca el **Panel**:

1. Inicie GFI LanGuard y haga clic en la ficha **Dashboard**.



Captura de pantalla 6: Visualización de Dashboard

2. En la lista de equipos, seleccione un equipo o un dispositivo móvil. La información del panel se actualiza según su selección.

4.3 Utilización del árbol de equipos

GFI LanGuard incluye opciones de filtrado y agrupación que le permiten encontrar rápidamente un equipo o dominio y visualizar de inmediato los resultados.

Cuando se seleccionan un equipo o grupo en el árbol de equipos, los resultados del panel se actualizan de forma automática. Presione **CTRL** y seleccione varios equipos para visualizar los resultados de equipos específicos.

Las siguientes son funciones que admite el árbol de equipos:

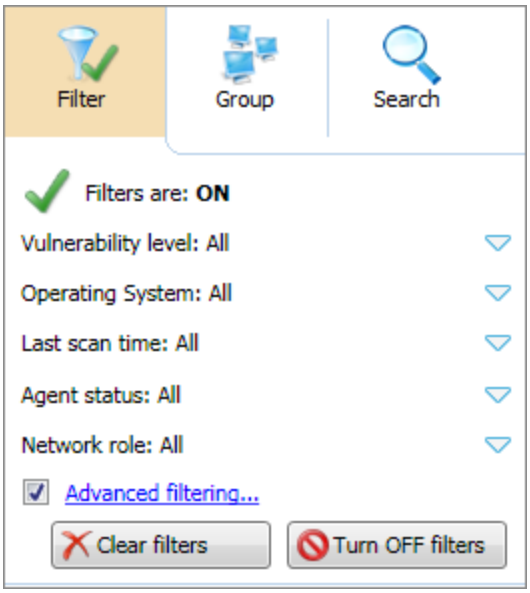
- Filtrado simple
- Filtrado avanzado
- Agrupando
- Búsqueda
- Sincronización con Active Directory

4.3.1 Filtrado simple

Para realizar el filtrado para un equipo o grupo específicos:

1. En el panel izquierdo, haga clic en **Filter**.

2. Configure los criterios y haga clic en **Turn ON filters**.

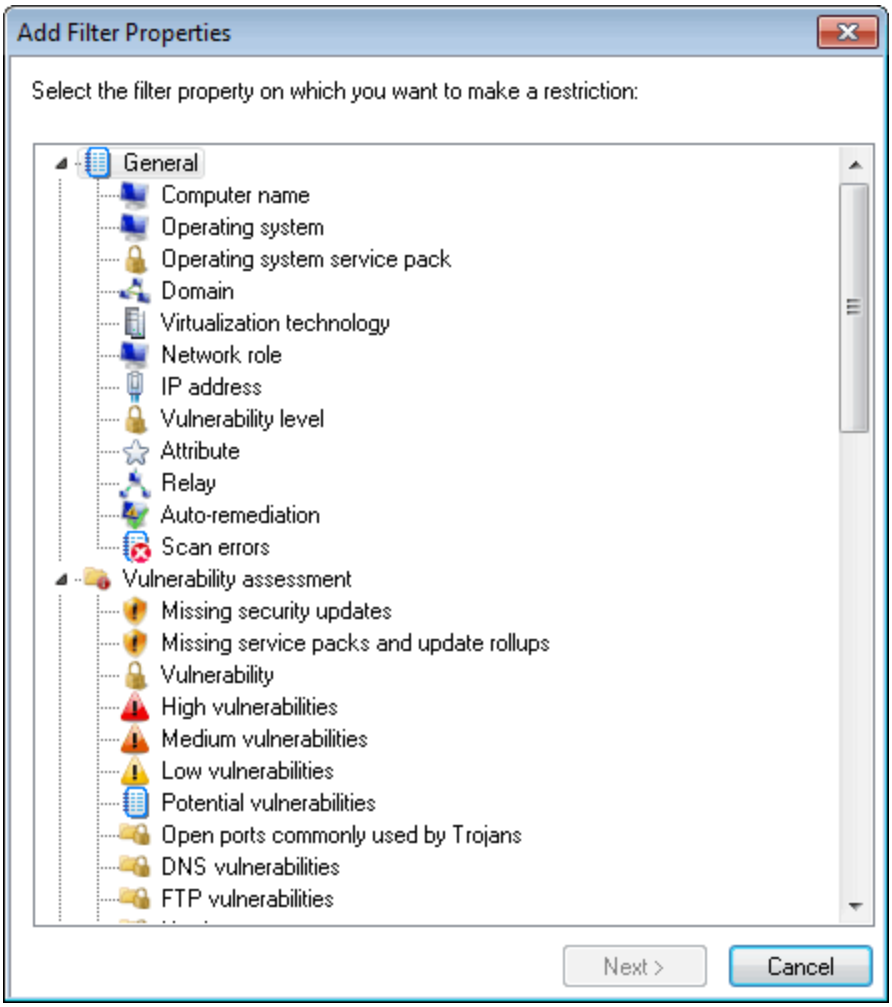


Captura de pantalla 7: Filtrado simple

4.3.2 Filtrado avanzado

Para realizar el filtrado para un equipo o grupo específicos utilizando el filtrado avanzado:

1. En el panel izquierdo, haga clic en **Filter** y en **Advanced filtering...**
2. En el cuadro de diálogo **Advanced Filtering**, haga clic en **Add**.



Captura de pantalla 8: Adición de propiedades de filtro

3. Seleccione la propiedad de filtro para la restricción y haga clic en **Next**.

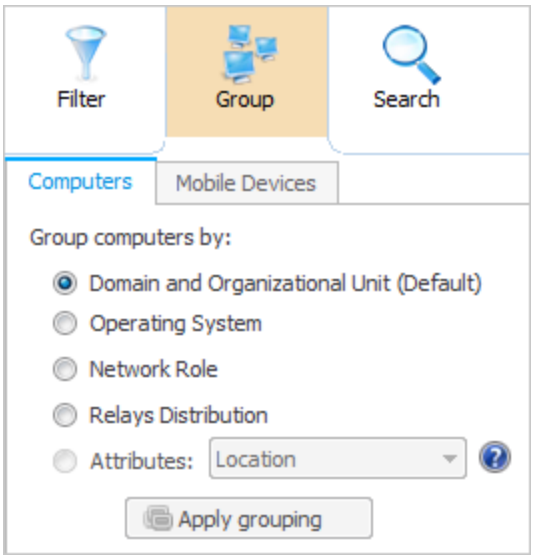
4. Seleccione la condición y escriba el valor de esta. Haga clic en **OK**.

5. Repita los pasos 2 a 4 para cada condición. Haga clic en **OK**.

4.3.3 Agrupando

Para agrupar equipos por atributos específicos:

1. En el panel izquierdo, haga clic en **Group**.



Captura de pantalla 9: Agrupando

2. Haga clic en una de las siguientes fichas y seleccione un atributo específico:

Fichas	Attributes
Computers (equipos)	» Domain and Organizational Unit » Sistema operativo » Network Role » Relays Distribution » Attributes
Mobile Devices (dispositivos móviles)	» Cuenta de usuario » Sistema operativo » Modelo de dispositivo » Attributes

Nota

Si se selecciona **Attributes**, elija el atributo de la lista desplegable. Para obtener más información, consulte Utilización de atributos (página 29).

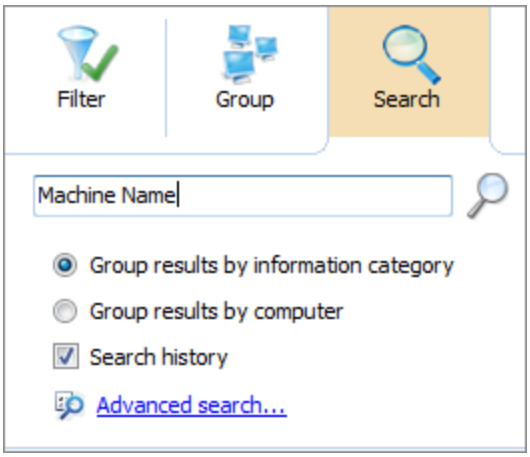
Si se selecciona Attributes, elija el atributo de la lista desplegable.

4. Haga clic en **Apply grouping**.

4.3.4 Búsqueda

La ficha Search de **Computers tree** le permite buscar y hacer que aparezcan resultados para un equipo o grupo específicos. Para que aparezcan resultados para un equipo específico:

1. En el **árbol de equipos**, seleccione **Search**.



Captura de pantalla 10: Búsqueda de equipos y grupos específicos

2. Escriba los criterios o de búsqueda y utilice las siguientes opciones:

Tabla 12: Opciones de búsqueda

Opción	Descripción
Group results by information category	Los resultados de búsqueda se agrupan por categoría. El resultado contiene la información de equipos más reciente. Entre otros eventos, los resultados se agrupan por: » Información sobre equipos » Dispositivos de hardware » Usuarios de la sesión actual » Procesos » Tecnología virtual
Group results by computer	Los resultados de búsqueda se agrupan por nombre de equipo. El resultado contiene la información de equipos más reciente.
Search History	Los resultados de búsqueda incluyen la información de exámenes previos.
Advanced search	Configure opciones de búsqueda avanzadas. **Nota** Para obtener más información, consulte la sección **Búsqueda de texto completo** de la **Guía del administrador**.

4.3.5 Sincronización con Active Directory

Esta característica le permite realizar las siguientes tareas:

- Agregar equipos que están en Active Directory pero no en GFI LanGuard aún.
- Mover equipos a la unidad organizativa correcta en el árbol de equipos de GFI LanGuard.
- Quitar equipos que han sido eliminados de Active Directory pero aún se encuentran enGFI LanGuard.

1. Haga clic con el botón derecho en el árbol de equipos que desea sincronizar y seleccione **Synchronize with Active Directory**.

2. Si aparecen, ingrese las credenciales de dominio necesarias para recuperar las unidades organizativas del dominio y haga clic en **OK**.

3. Haga clic en **Next** para iniciar el proceso de sincronización.

4. En la lista de equipos detectados, revise la lista de cambios que este proceso implementará. En dicha lista se indica en qué unidades organizativas de Active Directory se reubicará cada equipo. Haga clic en **Next**.

5. Revise la lista de equipos de Active Directory que se agregarán a GFI LanGuard. Haga clic en **Next**.

6. Revise la lista de equipos que ya no están presentes o que han sido eliminados de Active Directory. Haga clic en **Sync**.

7. Una vez finalizado el proceso, haga clic en **Finish**.

4.4 Utilización de atributos

Los atributos le permiten agrupar y configurar equipos de forma individual o grupal en una sola operación. También le permiten corregir vulnerabilidades o implementar software en equipos específicos según el atributo asignado. Las secciones siguientes contienen información sobre lo que se muestra a continuación:

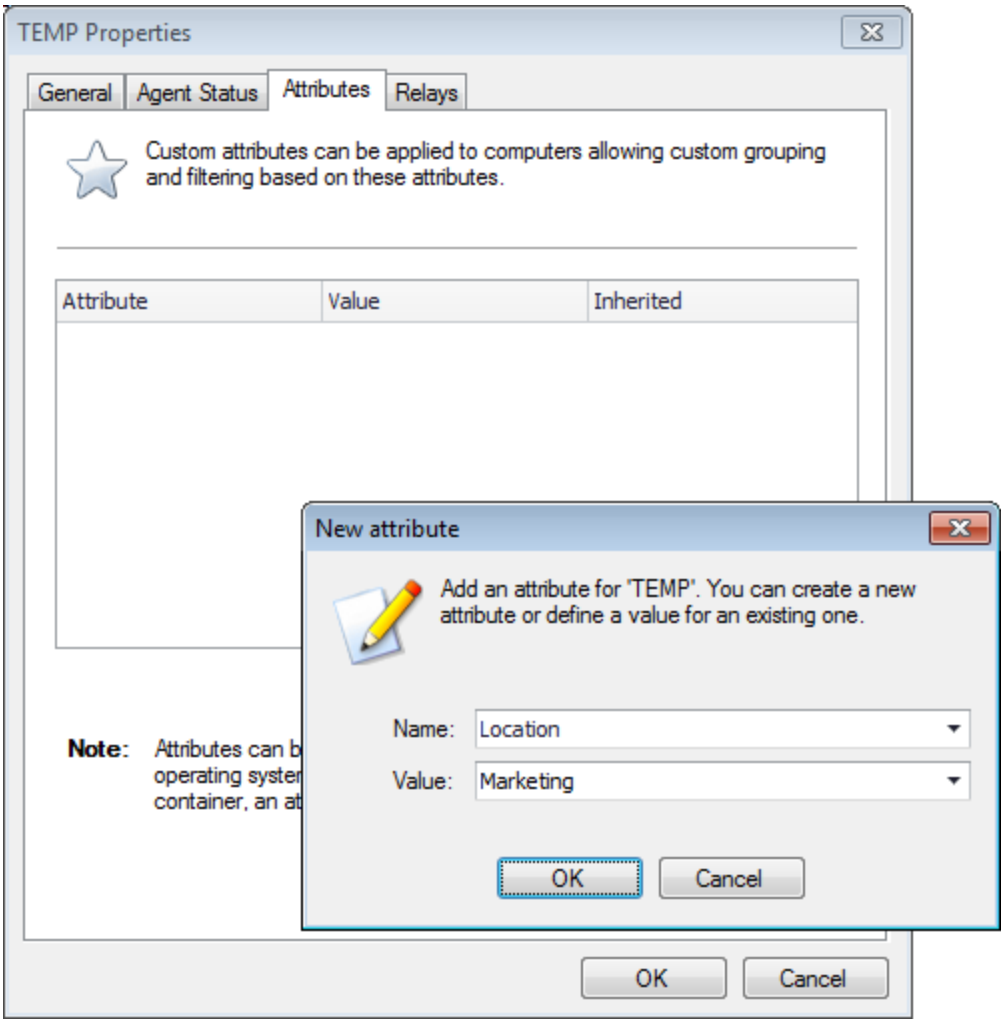
- Asignación de atributos a un equipo
- Asignación de atributos a un grupo
- Configuración de atributos

4.4.1 Asignación de atributos a un equipo

Para asignar atributos a un solo equipo:

1. Haga clic en la ficha **Dashboard**.

2. En el árbol de equipos, haga clic con el botón secundario en un equipo y seleccione **Assign attributes**.



Captura de pantalla 11: Asignación de atributos: Equipo único

3. En el cuadro de diálogo de **Propiedades**, ficha **Attributes**, haga clic en **Add**.

4. Configure parámetros de atributos nuevos y haga clic en **OK**.

5. Haga clic en **OK** para guardar su configuración.

4.4.2 Asignación de atributos a un grupo

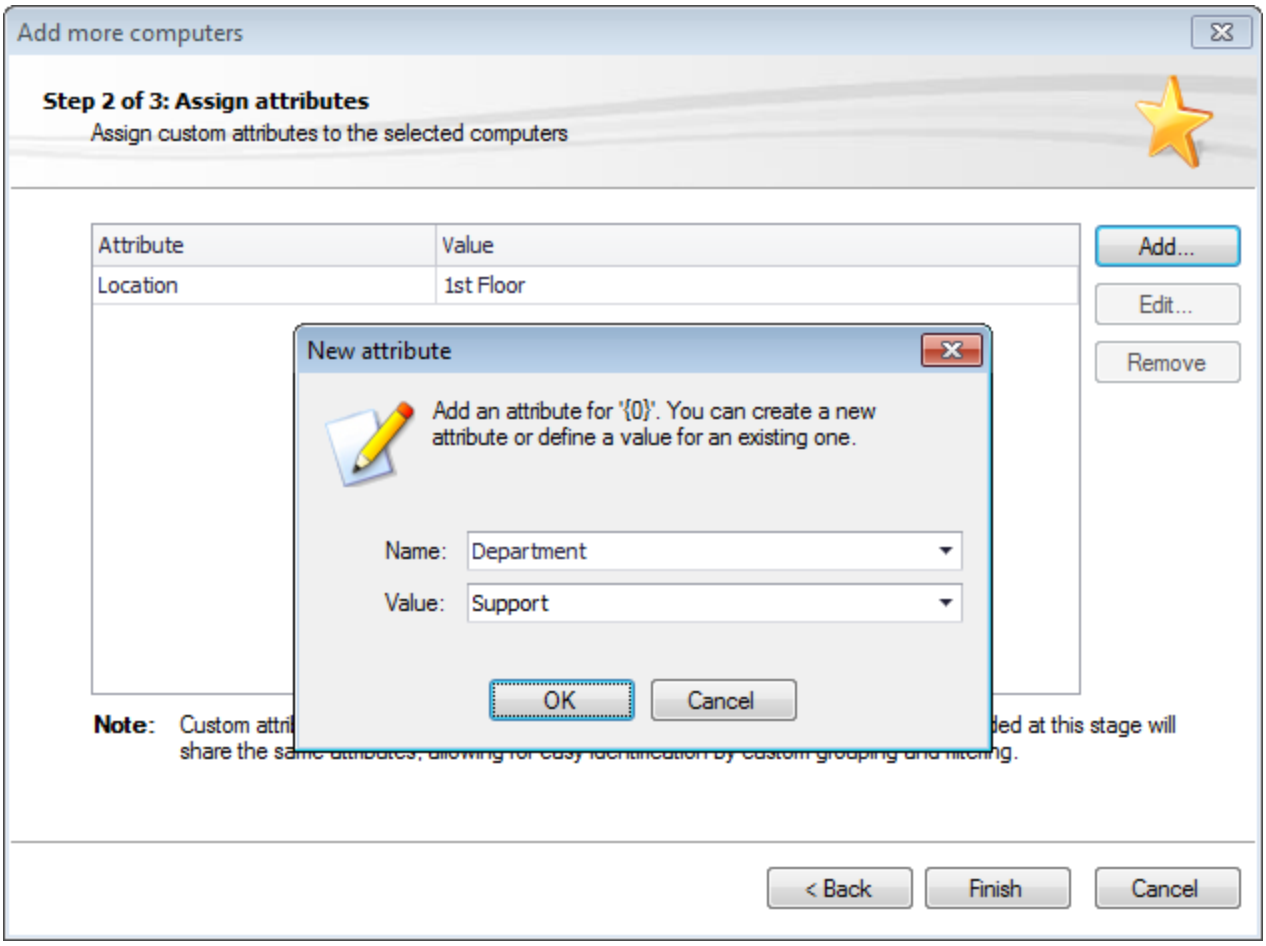
GFI LanGuard le permite asignar atributos a grupos, dominios unidades organizativas y redes en particular. Una vez asignados los atributos, cada miembro del grupo seleccionado hereda los parámetros de atributos.

Para asignar atributos a un grupo:

1. Haga clic en la ficha **Dashboard**.

2. En la lista de equipos, haga clic con el botón secundario en una red y seleccione **Assign attributes**.

3. En el asistente **Add more computers**, seleccione la red y haga clic en **Next**.



Captura de pantalla 12: Asignación de atributos: varios equipos

4. Haga clic en **Add** y configure los atributos correspondientes. Utilice los botones **Edit** y **Remove** para editar o quitar los atributos seleccionados.

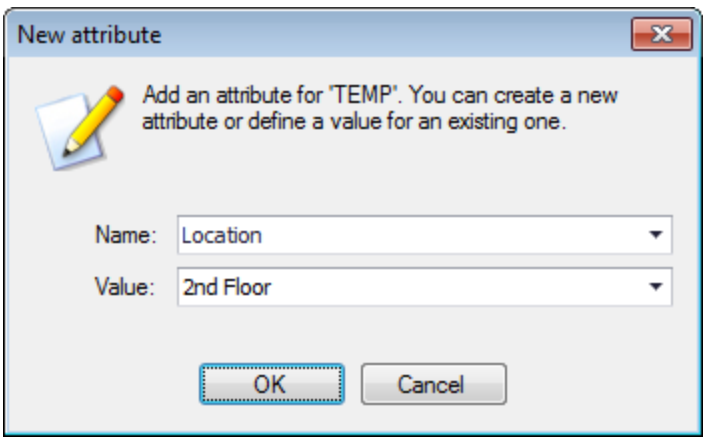
5. Haga clic en **Finish** para guardar su configuración.

4.4.3 Configuración de atributos

Para configurar atributos:

1. En el cuadro de diálogo **Properties**, haga clic en la ficha **Attributes**.

2. Haga clic en **Add** para iniciar el cuadro de diálogo **New attribute**.



Captura de pantalla 13: Cuadro de diálogo de nuevo atributo

3. En el menú desplegable de **Name**, seleccione un atributo o escriba un nombre para crear uno nuevo.

4. Especifique un valor para el atributo en el campo **Value**. Haga clic en **OK**.

Repita los pasos 2 a 4 hasta añadir todos los atributos requeridos.

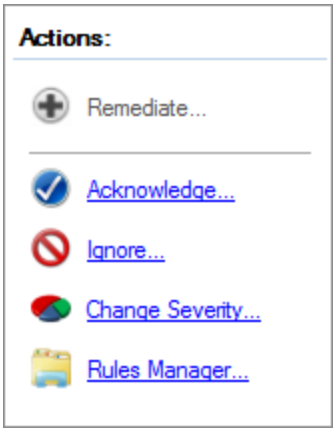
6. Haga clic en **OK** para guardar su configuración.

4.5 Acciones del panel

La sección **Actions** le permite administrar y corregir vulnerabilidades y revisiones faltantes halladas en su red. Para acceder a la sección **Actions**:

1. Seleccione la ficha **Dashboard**.

2. Haga clic en la ficha **Vulnerabilities** o **Patches**.



Captura de pantalla 14: Sección Actions de Dashboard

3. Seleccione una de las siguientes acciones:

Tabla 13: Acciones del panel

Acción	Descripción
Remediate	Permite iniciar Remediation Center para implementar y administrar revisiones faltantes.
Acknowledge	Inicia el cuadro de diálogo Rule-Acknowledge Patch. Esto le permite confirmar problemas para que estos no afecten el nivel de vulnerabilidad de su red. Determine mediante configuración para qué equipo se aplica esta regla.
Ignore	Inicia el cuadro de diálogo Rule-Ignore Patch. Esto le permite ignorar revisiones faltantes o vulnerabilidades para que estas no se informen como problemas en el futuro, e incluir razones por las cuales tales vulnerabilidades se deben ignorar. Determine mediante configuración para qué equipo se aplica esta regla y el periodo de tiempo durante el cual se ignora el problema.
Change Severity	Inicia el cuadro de diálogo Rule-Change Severity. Esto le permite cambiar el nivel de gravedad de la vulnerabilidad. Determine mediante configuración para qué equipos se aplica esta regla y también el nivel de gravedad.
Rules Manager	Inicia el cuadro de diálogo Rules Manager. Esto le permite buscar y quitar reglas configuradas y visualizar las razones para ignorar revisiones faltantes y vulnerabilidades.

4.6 Exportación de la lista de problemas

GFI LanGuard le permite exportar listas de problemas al formato de documento portátil de Adobe (PDF), a Microsoft Office Excel (XLS) o al lenguaje de marcado de hipertexto (HTML). Cuando una lista admite la exportación, los iconos aparecen en la esquina superior derecha de la lista. Seleccione el icono correspondiente y configure los parámetros de exportación.

4.7 Vistas del panel

El panel de GFI LanGuard consta de varias vistas. Estas vistas diferentes le permiten controlar en tiempo real sus destinos de examen y realizar operaciones de corrección e informe al instante. Las secciones siguientes contienen información sobre lo que se muestra a continuación:

- Overview de Dashboard
- Vista Computers
- Vista History
- Vista de Vulnerabilities
- Vista Patches
- Vista Ports
- Vista Software
- Vista Hardware
- Vista System Information

4.7.1 Información general

Captura de pantalla 15: Información general del panel

Overview, en Dashboard, es una representación gráfica del nivel de seguridad y de vulnerabilidad de un único equipo o dominio, o bien de una red completa.

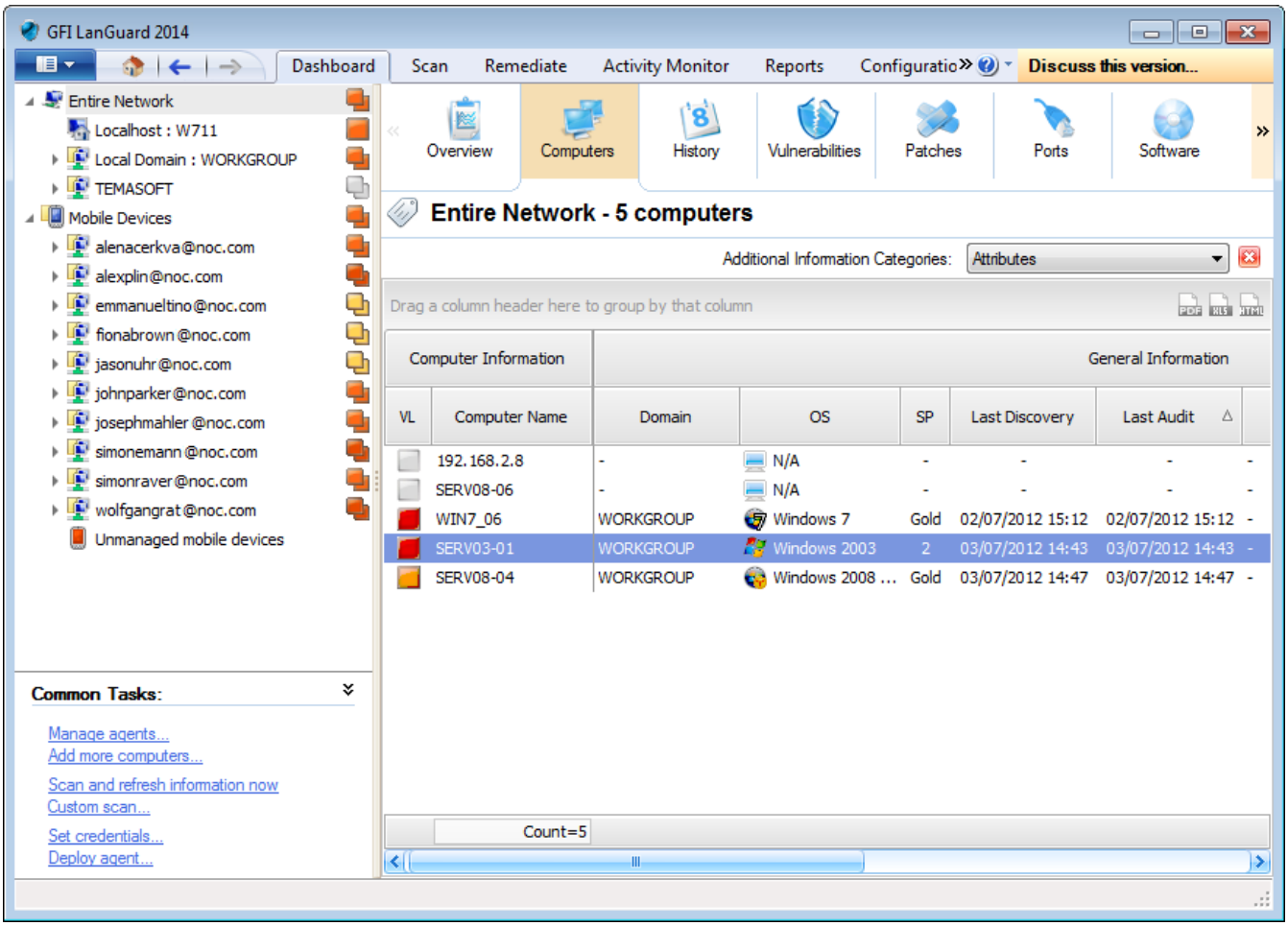
Cuando un equipo o dominio se seleccionan, los resultados relacionados con estos se actualizan de forma automática en el panel. A continuación se ofrece una descripción de cada sección del panel:

Tabla 14: Información de software de una auditoría

Sección	Descripción
Network security level	Esta valoración indica el nivel de vulnerabilidad de un equpo o una red, según el número y el tipo de vulnerabilidades o revisiones que se encuentren. Un nivel de vulnerabilidad alto es el resultado de vulnerabilidades o de revisiones faltantes cuya severidad promedio es de categoría alta.
Computer vulnerability distribution	Este gráfico se encuentra disponible únicamente cuando se seleccionan un dominio o grupo de trabajo, y muestra la distribución de vulnerabilidades en su red. Este gráfico le permite determinar cuántos equipos tienen una clasificación de vulnerabilidad alta, media o baja.
Most vulnerable computers	Este gráfico se encuentra disponible únicamente cuando se seleccionan un dominio o grupo de trabajo, y muestra los equipos más vulnerables detectados durante el examen. El color del icono de la izquierda indica el nivel de vulnerabilidad.
Agent Status	Cuando se seleccionan un dominio o grupo de trabajo, aparece un gráfico que muestra el estado de agentes general de todos los equipos dentro del dominio o grupo de trabajo. Esto le permite determinar el número de agentes instalados o las instalaciones pendientes en el dominio o grupo de trabajo seleccionados. Cuando se selecciona un equipo, esta sección muestra un icono que representa el estado de agentes. Los iconos se describen a continuación: » **No instalado**: el agente no se ha instalado en el equipo de destino. » **Instalación pendiente**: la instalación está pendiente. El estado puede ser “pendiente” cuando el equipo se encuentra fuera de línea o la instalación del agente está en curso. » **Desinstalación pendiente**: la desinstalación está pendiente. El estado puede ser “pendiente” cuando el equipo se encuentra fuera de línea o la desdesinstalar del agente está en curso. » **Instalado**: el agente está instalado en el equipo de destino. » **Agente de retransmisión instalado**: los equipos seleccionados son agentes de retransmisión.
Audit status	Este gráfico se encuentra disponible cuando se seleccionan un dominio o un grupo de trabajo, y le permite determinar cuántas auditorías, agrupadas por hora, se han realizado en su red.
Vulnerability trends over time	Cuando se seleccionan un dominio o grupo de trabajo, en esta sección aparece un gráfico de línea que muestra el cambio del nivel de vulnerabilidad, agrupado por conteo de equipos, en función del tiempo. Cuando se seleccionan un dominio o grupo de trabajo, en esta sección aparece un gráfico que muestra el cambio del nivel de vulnerabilidad en función del tiempo para el equipo seleccionado.
Computers by network role	Este gráfico se encuentra disponible únicamente cuando se seleccionan un dominio o grupo de trabajo, y muestra el número de equipos auditados, agrupados por rol de red. Entre otros roles, este gráfico identifica el número de servidores y estaciones de trabajo por dominio seleccionado.
Computers by operating system	Este gráfico se encuentra disponible únicamente cuando se seleccionan un dominio o grupo de trabajo, y muestra el número de equipos auditados, agrupados por sistema operativo instalado.
Computer details	Esta sección se encuentra disponible cuando se selecciona un solo equipo y le permite ver los detalles de este.

Sección	Descripción
Scan activity	Este gráfico de línea se encuentra disponible únicamente cuando se selecciona un solo equipo y le permite ver el número de exámenes o auditorías que se realicen en el equipo seleccionado. A su vez, le permite verificar si se realizan exámenes programados.
Remediation Activity	Este gráfico de línea se encuentra disponible únicamente cuando se selecciona un solo equipo y le permite ver el número de actividades de corrección que se realicen en el equipo seleccionado. Además, este gráfico le permite verificar que se realice la corrección automática.
Top 5 Issues to Address	Esta sección se encuentra disponible cuando se selecciona un solo equipo y muestra los cinco problemas principales que se deben abordar para el equipo seleccionado.
Results statistics	Esta sección se encuentra disponible cuando se selecciona un solo equipo y muestra información general del resultado de la auditoría. Entre otras posibilidades, el resultado le permite identificar el número de revisiones faltantes y de aplicaciones instaladas, los puertos abiertos y los servicios en ejecución.
Security Sensors	Esta sección le permite identificar problemas de un vistazo. Haga clic en un sensor para recorrer y mostrar los problemas y las vulnerabilidades para un equipo o grupo específicos. Los sensores le permiten identificar: » Actualizaciones de software faltantes » Service Pack faltantes » Vulnerabilidades » Problemas en cortafuegos » Aplicaciones no autorizadas » Estado de auditorías » Configuración de credenciales » Problemas de protección de malware » Problemas de estado de agentes

4.7.2 Vista Computers



Captura de pantalla 16: Resultados de análisis por equipo

Seleccione esta vista para realizar auditorías en grupo de los resultados por equipo. En la lista desplegable, seleccione una de las opciones descritas a continuación:

Tabla 15: Vista según la información de los equipos

Opción	Descripción
Agent Details	Seleccione esta opción para ver el estado de agentes. Esta opción le permite determinar si hay instalado un agente en un equipo y, si esto sucede, muestra el tipo de credenciales utilizadas por el agente.
Vulnerabilities	Permite ver el número de vulnerabilidades de un equipo agrupadas por gravedad. La gravedad de una vulnerabilidad puede ser: » Alta » Media » Baja » Potential.
Patching status	Vea el número de: » Actualizaciones de seguridad y no de seguridad faltantes » Service Pack y paquetes acumulativos de actualizaciones faltantes » Actualizaciones de seguridad y no de seguridad instaladas » Service Pack y paquetes acumulativos de actualizaciones instalados.

Opción	Descripción
Open ports	Vea el número de: » Puertos TCP abiertos » Puertos UDP abiertos » Puertas traseras.
Software	Vea el número de: » Motores de protección contra la suplantación de identidad » Motores antispyware » Motores antivirus » Aplicaciones de copia de seguridad » Aplicaciones de prevención contra pérdida de datos » Aplicaciones de acceso a dispositivos y cifrado de discos » Cortafuegos » Aplicaciones instaladas » Aplicaciones de mensajería instantánea » Aplicaciones entre pares » Aplicaciones no autorizadas » Equipos virtuales » Clientes de VPN » Exploradores web.
Hardware	Vea información sobre lo siguiente: » Número de unidades de disco » Espacio libre en disco » Tamaño de la memoria » Número de procesadores » Otro hardware.
System information	Vea información sobre lo siguiente: » El número de carpetas compartidas » Número de grupos » Número de usuarios » Usuarios de la sesión actual » Estado de la directiva de auditoría.
Attributes	Agrega una columna **Attributes** y agrupa sus destinos de examen según el atributo asignado.

Nota

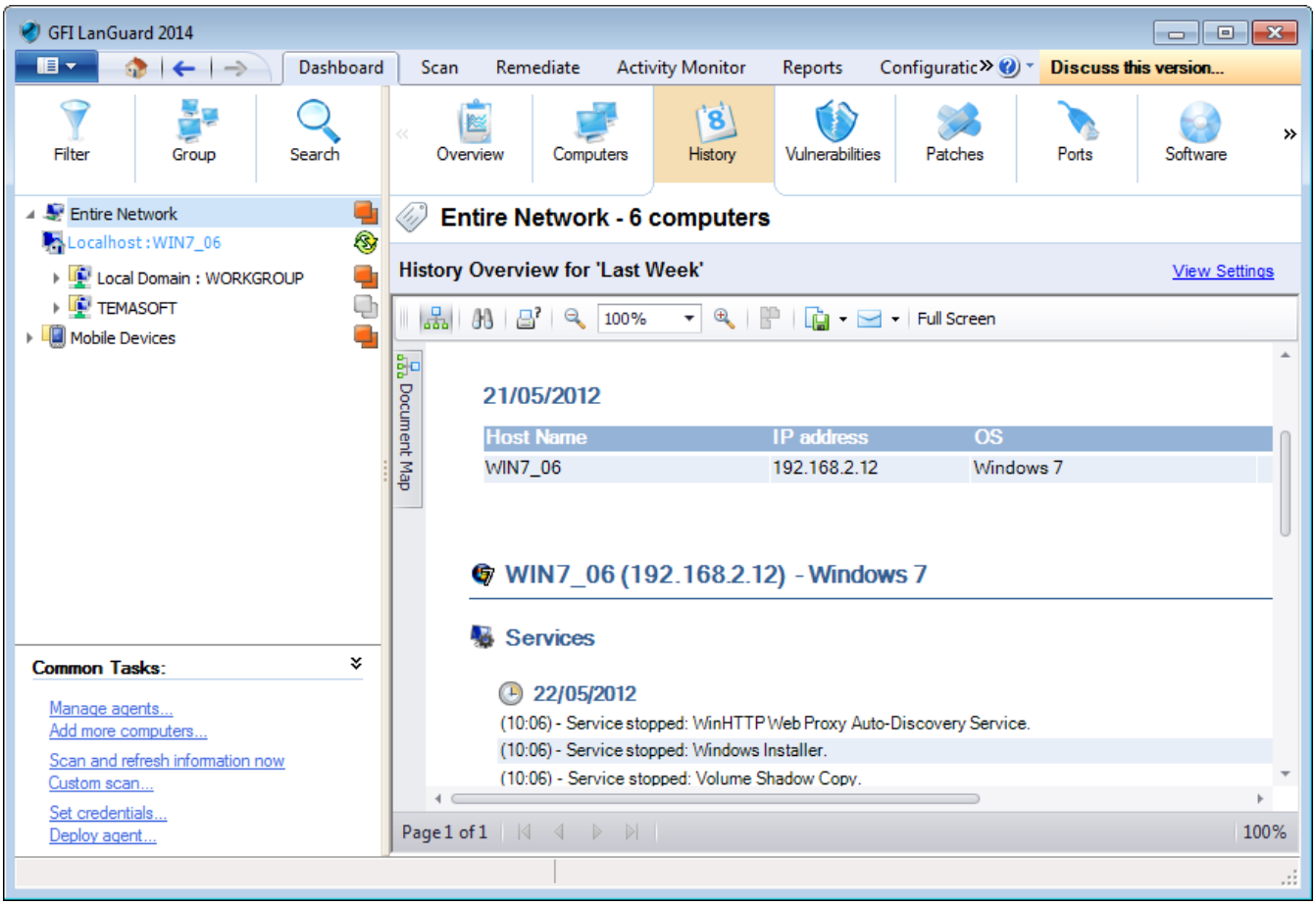
Para la iniciar la ficha **Overview** y visualizar más detalles de un equipo específico, haga doble clic en un equipo de la lista.

Nota

Arrastre y suelte un encabezado de columna en el área designada para agrupar datos por criterios.

4.7.3 Vista History

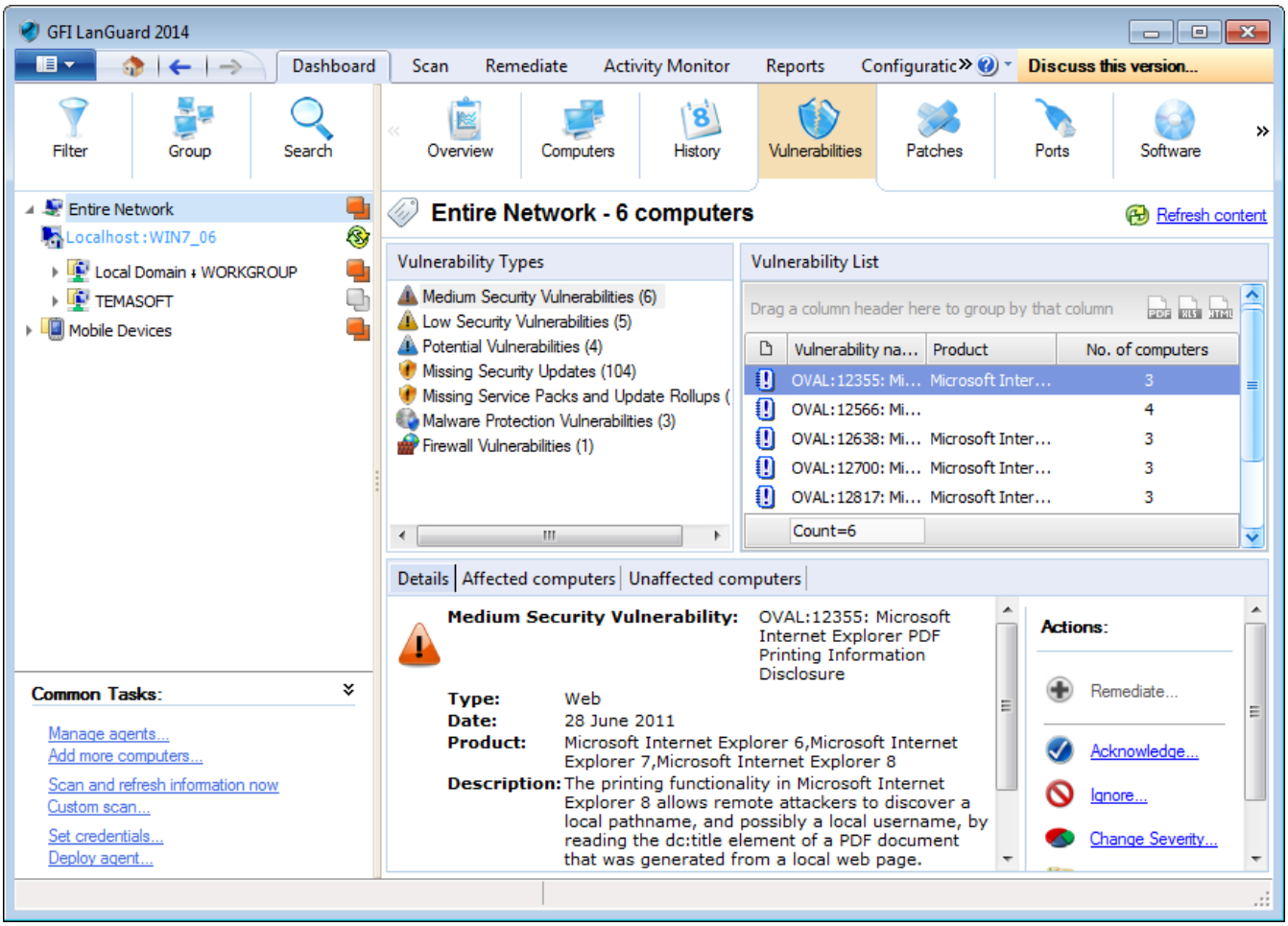
Seleccione esta vista para agrupar resultados de auditoría por fecha para un equipo específico. Para configurar la fecha de inicio del historial o el periodo del historial, haga clic en el enlace proporcionado.



Captura de pantalla 17: Vista History de Dashboard

4.7.4 Vista Vulnerabilities

Permite visualizar más detalles acerca de las vulnerabilidades halladas en una red y el número de equipos afectados. Cuando se selecciona una vulnerabilidad en la lista de **Vulnerability**, en la sección **Details** se proporciona más información sobre la vulnerabilidad seleccionada. En la sección **Details** (detalles) haga clic en **Affected computers** (equipos afectados) o en **Unaffected computers** (equipos no afectados) para que aparezca una lista de equipos afectados y no afectados.



Captura de pantalla 18: Vista Vulnerabilities de Dashboard

> **Nota**
>
> Arrastre y suelte un encabezado de columna en el área designada para agrupar datos por criterios.

4.7.5 Configuración de acciones

En la sección Actions, seleccione una de las descritas a continuación para administrar y corregir vulnerabilidades y revisiones faltantes halladas en su red.

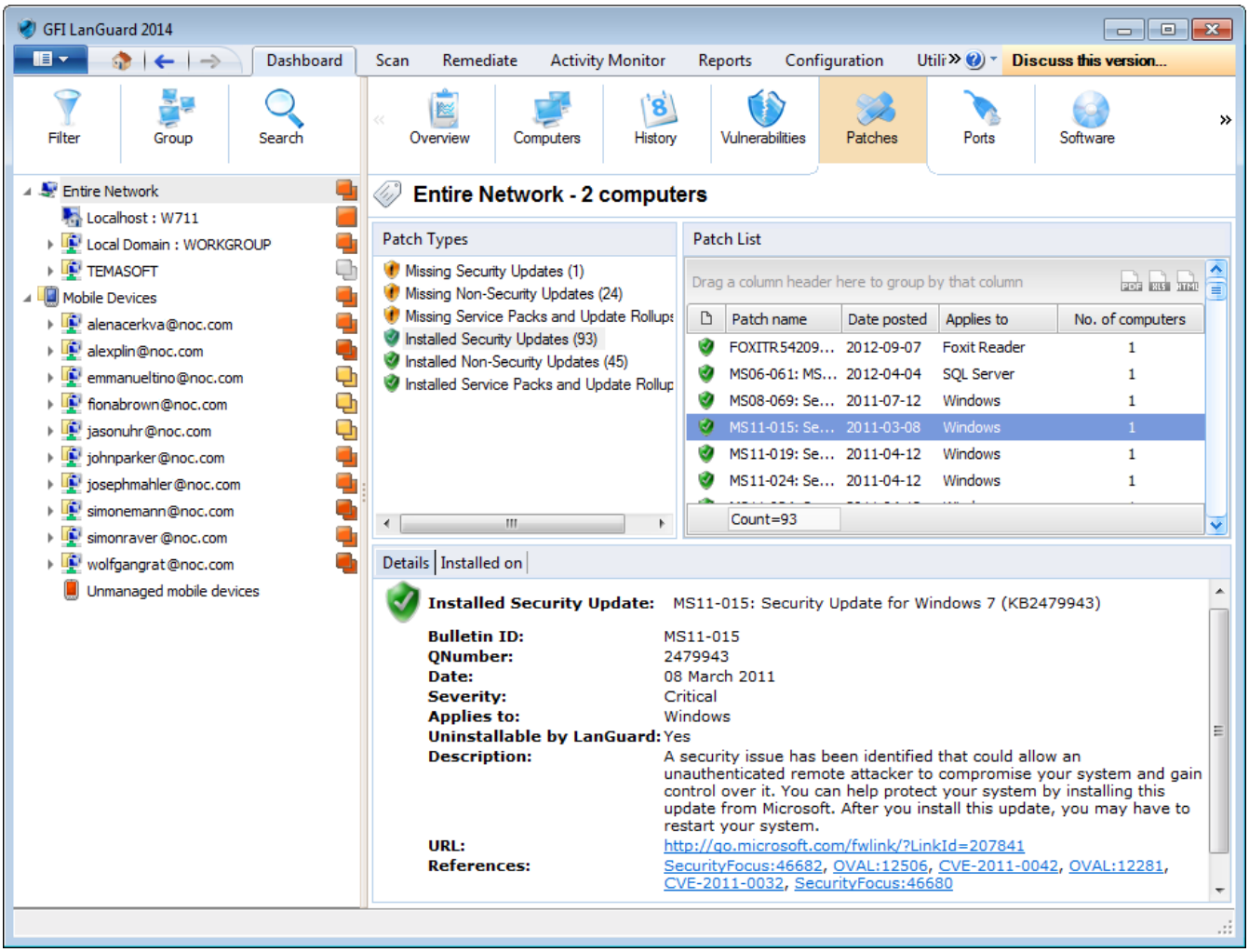
Tabla 16: Acciones del panel

Acción	Descripción
Remediate	Permite iniciar Remediation Center para implementar y administrar revisiones faltantes.
Acknowledge	Inicia el cuadro de diálogo Rule-Acknowledge Patch. Esto le permite confirmar problemas para que estos no afecten el nivel de vulnerabilidad de su red. Determine mediante configuración para qué equipo se aplica esta regla.

Acción	Descripción
Ignore	Inicia el cuadro de diálogo Rule-Ignore Patch. Esto le permite ignorar revisiones faltantes o vulnerabilidades para que estas no se informen como problemas en el futuro, e incluir razones por las cuales tales vulnerabilidades se deben ignorar. Determine mediante configuración para qué equipo se aplica esta regla y el periodo de tiempo durante el cual se ignora el problema.
Change Severity	Inicia el cuadro de diálogo Rule-Change Severity. Esto le permite cambiar el nivel de gravedad de la vulnerabilidad. Determine mediante configuración para qué equipos se aplica esta regla y también el nivel de gravedad.
Rules Manager	Inicia el cuadro de diálogo Rules Manager. Esto le permite buscar y quitar reglas configuradas y visualizar las razones para ignorar revisiones faltantes y vulnerabilidades.

4.7.6 Vista Patches

Permite mostrar más detalles relacionados con las revisiones y los Service Pack faltantes o instalados hallados durante una auditoría de red. Cuando se seleccionan una revisión o un Service Pack de la lista, la sección **Details** proporciona más información sobre la revisión o el Service Pack seleccionados. En la sección **Details**, haga clic en **Missing on** para que aparezca una lista de equipos para los que falte la revisión seleccionada.

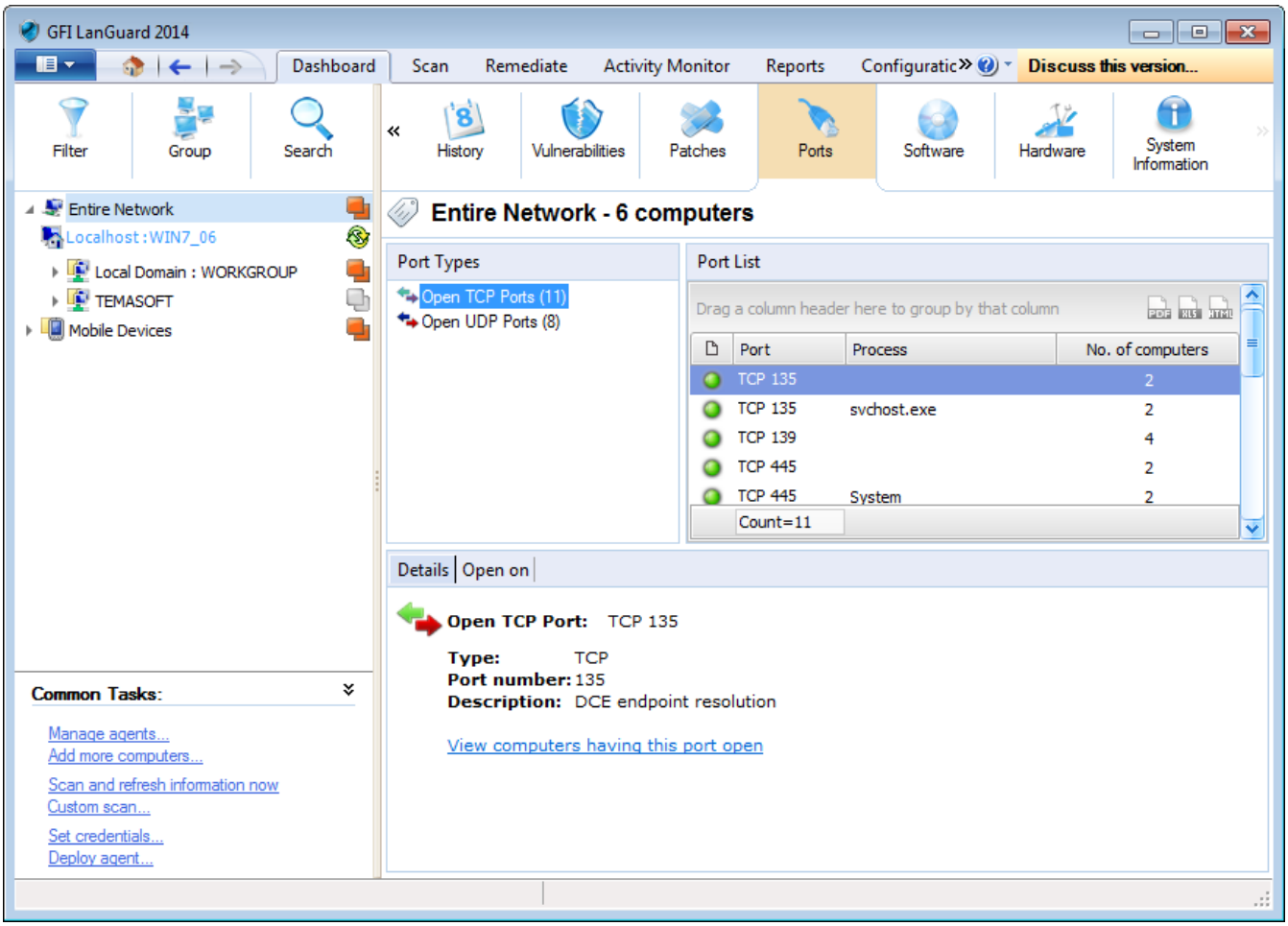


Captura de pantalla 19: Vista Patches de Dashboard

> **Nota**
>
> Arrastre y suelte un encabezado de columna en el área designada para agrupar datos por criterios.

4.7.7 Vista Ports

Permite mostrar más detalles relacionados con los puertos abiertos hallados durante una auditoría de red. Cuando se selecciona un puerto en la lista de **Port**, en la sección **Details** se proporciona más información sobre el puerto seleccionado. En la sección **Details**, haga clic en **View computers having this port open** para que aparezca una lista de equipos con el puerto seleccionado abierto.



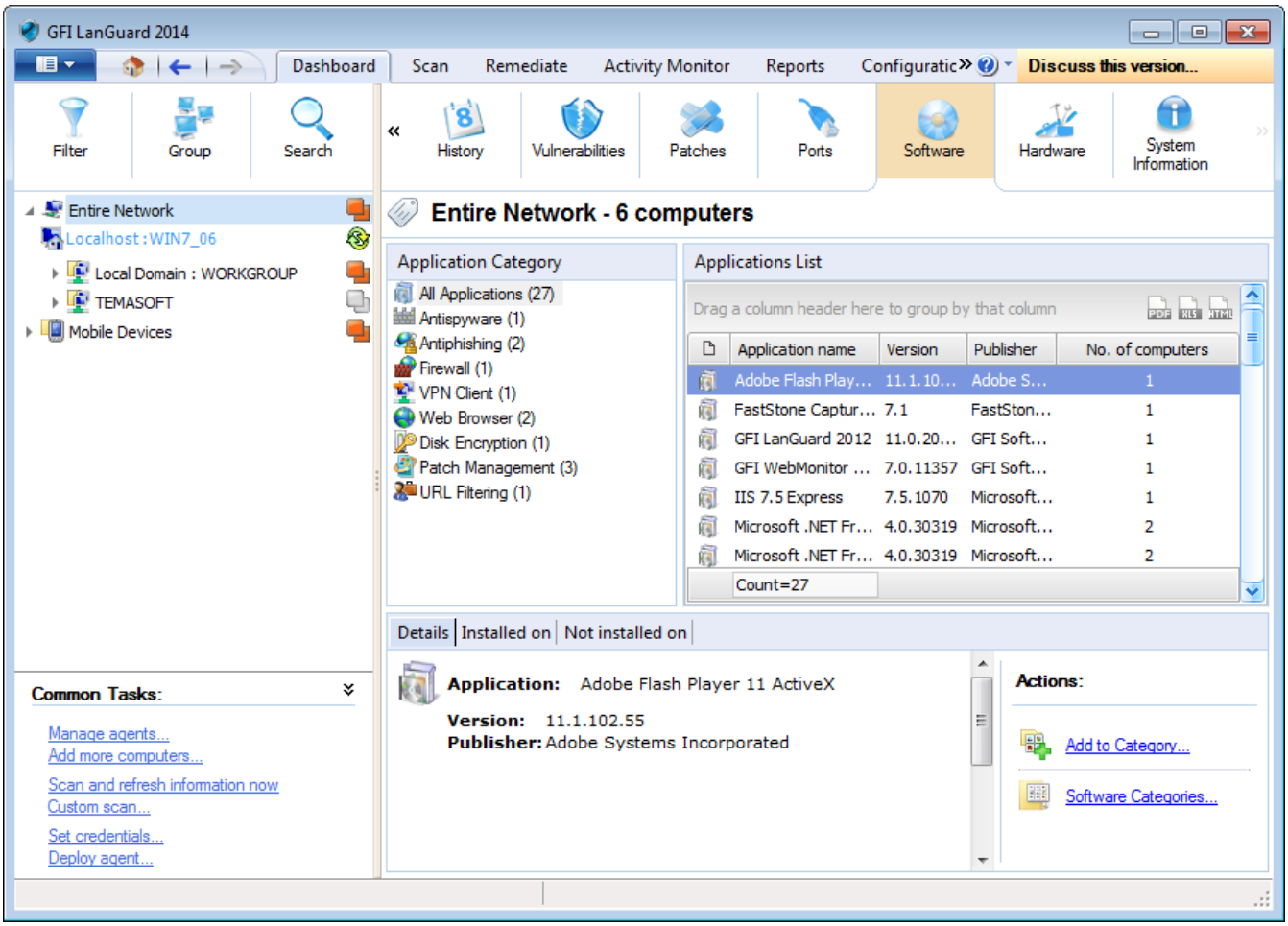
Captura de pantalla 20: Vista Ports de Dashboard

Nota

Arrastre y suelte un encabezado de columna en el área designada para agrupar datos por criterios.

4.7.8 Vista Software

Haga que se muestren más detalles relacionados con las aplicaciones instaladas halladas durante una auditoría de red. Cuando se selecciona una aplicación en la lista de **Application**, la sección **Details** proporciona más información sobre la aplicación seleccionada.



Captura de pantalla 21: Vista Software de Dashboard

En la sección Actions, seleccione una de las acciones descritas a continuación para administrar y categorizar aplicaciones de software.

Tabla 17: Acciones

Opción	Descripción
Add to category	Permite agregar aplicaciones a una categoría en particular
Software Categories	Permite configurar reglas para categorías de software y aplicaciones en particular. .

Nota

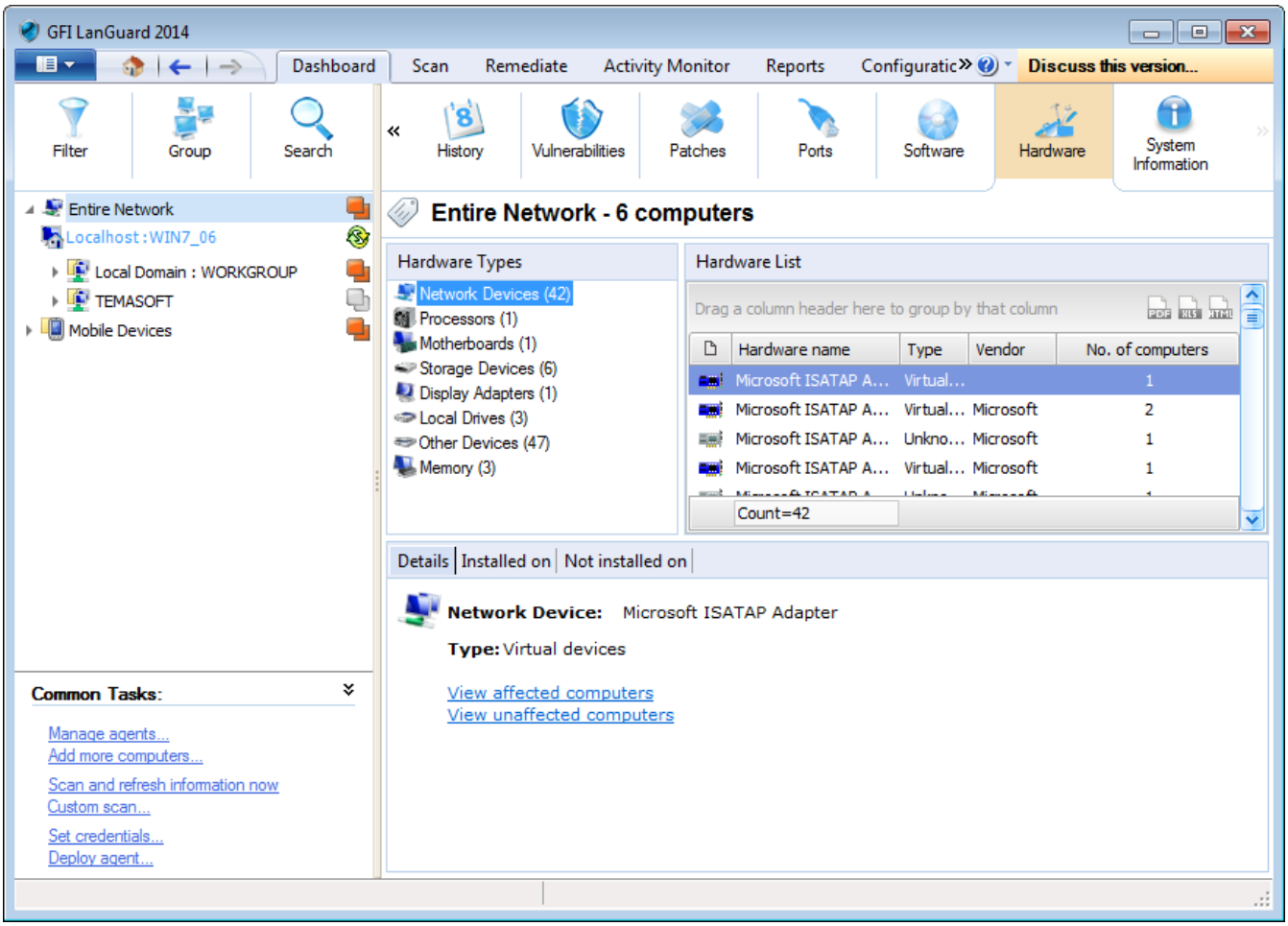
Arrastre y suelte un encabezado de columna en el área designada para agrupar datos por criterios.

Nota

Para los exámenes sin agente se requiere la ejecución temporal de un servicio en el equipo remoto. Seleccione **Habilitar auditoría completa de aplicaciones de seguridad…** para habilitar este servicio en todos los perfiles de examen sin agente.

4.7.9 Vista Hardware

Permite visualizar más nformación sobre el hardware hallado durante una auditoría de red. Seleccione el hardware de la lista para que se muestren más detalles.



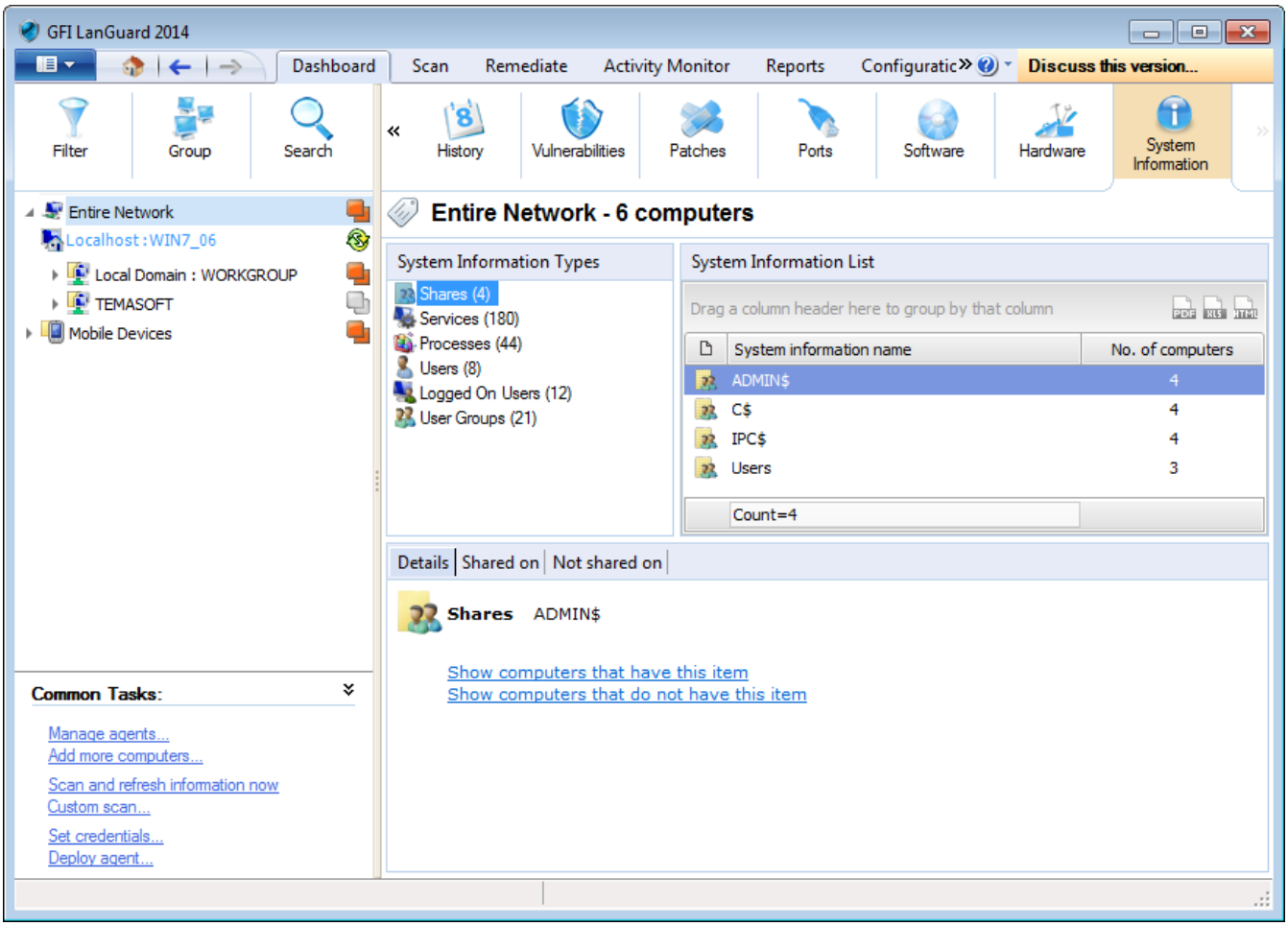
Captura de pantalla 22: Vista Hardware de Dashboard

Nota

Arrastre y suelte un encabezado de columna en el área designada para agrupar datos por criterios.

4.7.10 Vista System Information

En la ficha **System Information** se muestra información asociada con el sistema operativo de un destino de examen.



Captura de pantalla 23: Vista System Information de Dashboard

> **Nota**
>
> Arrastre y suelte un encabezado de columna en el área designada para agrupar datos por criterios.

5 Solución de problemas y asistencia técnica

En este capítulo se explica cómo solucionar problemas que se pueden encontrar durante la utilización de GFI LanGuard. Estos problemas se pueden resolver recurriendo al contenido de esta **Guía de instalación y configuración**. Si quedan problemas sin resolver después de revisar el manual, verifique si su problema se enumera a continuación.

Consulte las secciones siguientes para obtener información sobre cómo resolver problemas comunes y contactar al equipo de asistencia técnica.

Temas de este capítulo:

5.1 Resolución de problemas comunes 47
5.2 Utilización del asistente para el solucionador de problemas 49
5.3 GFI SkyNet 51
5.4 Foro web 51
5.5 Solicitud de asistencia técnica 51

5.1 Resolución de problemas comunes

En la siguiente tabla se le proporcionan soluciones para los problemas más comunes que puede encontrar al utilizar GFI LanGuard:

Tabla 18: Problemas comunes de GFI LanGuard

Problema hallado	Solución/Descripción
Se encuentra el error **Failed to connect to database** al intentar configurar el back-end de base de datos.	**Descripción** Este problema se puede producir cuando se cumplen las dos condiciones siguientes: 1. GFI LanGuard se instala en Windows 2000 SP4 con MDAC 2.5 SP 3 2. El back-end de base de datos es SQL Server® y tiene un nombre de instancia de base de datos que difiere del nombre del equipo con SQL Server®. **Solución** Instale **Microsoft® Data Access Components** (MDAC, 2.6 o posterior) en el equipo con GFI LanGuard y realice un nuevo intento. MDAC se puede descargar desde: http://go.gfi.com/?pageid=download_mdac
The database structure is incorrect. Do you want to delete and recreate the database? Esta advertencia se encuentra al intentar configurar el back-end de base de datos.	**Descripción** Este problema se produce cuando la estructura de la base de datos está dañada. O bien La base de datos devuelve un vencimiento de tiempo de espera debido a que la conexión no se puede establecer. **Solución** Cuando aparezca este mensaje: Verifique que todas las credenciales de SQL sean correctas y que no existan problemas de conectividad entre el equipo con GFI LanGuard y SQL Server. Es importante tener en cuenta que cuando se hace clic en OK todos los exámenes guardados se pierden.

Problema hallado	Solución/Descripción
Se encuentra el error Failed to connect to database al intentar acceder a la ficha Change database mientras se configura la base de datos SQL.	**Descripción** Este problema se puede producir cuando se cumplen las dos condiciones siguientes: » GFI LanGuard se instala en Windows 2000 SP4 con MDAC 2.5 SP 3 » El back-end de base de datos es SQL Server® y tiene un nombre de instancia de base de datos que difiere del nombre del equipo con SQL Server®. **Solución** Instale Microsoft® Data Access Components (MDAC, 2.6 o posterior) en el equipo con GFI LanGuard y realice un nuevo intento. **Nota** MDAC se puede descargar desde: http://go.gfi.com/?pageid=download_mdac
Resultados incompletos y errores al examinar equipos remotos	**Descripción** Se pueden encontrar errores similares a los siguientes: » Failed to open test key to remote registry » The scan will not continue » Access Denied » Could not connect to remote SMB server. Estos errores se pueden encontrar debido a que: » El equipo remoto tiene una cuenta similar a la utilizada por GFI LanGuard para iniciar sesión como administrador. » La cuenta de usuario utilizada por GFI LanGuard no tiene privilegios administrativos. **Solución** Para resolver este problema, realice una de las siguientes acciones: » Inicie sesión en el equipo con GFI LanGuard y configure GFI LanGuard para utilizar una cuenta de administrador de dominio alternativa. » Borre la cuenta de usuario local del equipo remoto. » Inicie GFI LanGuard ejecutándolo con “Run As” a través de una cuenta de administrador de dominio. **Nota** Para obtener más información, consulte http://go.gfi.com/?pageid=LAN_ProbScanningRM
Las actualizaciones de programa de GFI LanGuard no funcionan	**Descripción** Las actualizaciones no funcionarán si el equipo con GFI LanGuard no tiene una conexión directa a Internet. **Solución** Para resolver este problema, realice una de las siguientes acciones: » Configure el equipo con GFI LanGuard para que tenga acceso directo a Internet. » Instale otro GFI LanGuard en un equipo con acceso a Internet y configure GFI LanGuard para que busque actualizaciones en la nueva instalación. **Nota** Para obtener más información, consulte http://go.gfi.com/?pageid=LAN_CheckAltUpdates

Problema hallado	Solución/Descripción
El cortafuegos instalado en GFI LanGuard bloquea la conexión con los equipos de destino.	**Descripción** La detección podría perder velocidad o bloquearse si se instala un cortafuegos en el equipo con GFI LanGuard. **Solución** Configure el cortafuegos para que permita los siguientes componentes en conexiones salientes: » <..\Program Files\GFI\LanGuard>*.exe » <..\Program Files\GFI\LanGuard Agent>*.exe **Nota** Para obtener más información, consulte http://go.gfi.com/?pageid=LAN_SetBestPerformance
GFI LanGuard no puede recuperar los equipos del grupo de trabajo cuando se utiliza Enumerate Computers	**Descripción** GFI LanGuard utiliza el mecanismo de Windows para recuperar equipos dentro de un grupo de trabajo. En este mecanismo, un equipo examinador principal creará y almacenará una lista de todos los equipos. En algunos casos, el rol de examinador principal puede exhibir errores que pueden hacer que GFI LanGuard no obtenga la información de los equipos. **Nota** Para solucionar este problema, consulte http://go.gfi.com/?pageid=LAN_CannotEnumerate
GFI LanGuard encontró puertos abiertos que otro detector encontró cerrados	**Descripción** GFI LanGuard utiliza un enfoque diferente del de otros detectores de puertos para detectar puertos abiertos. **Solución** Para ver el estado de un puerto y determinar si está cerrado o abierto: 1. Haga clic en **Inicio > Programas > Accesorios > Símbolo del sistema**. 2. Escriba `netstat -an` y presione **Entrar**. 3. En la lista que se genera se muestran todas las conexiones activas de equipos.

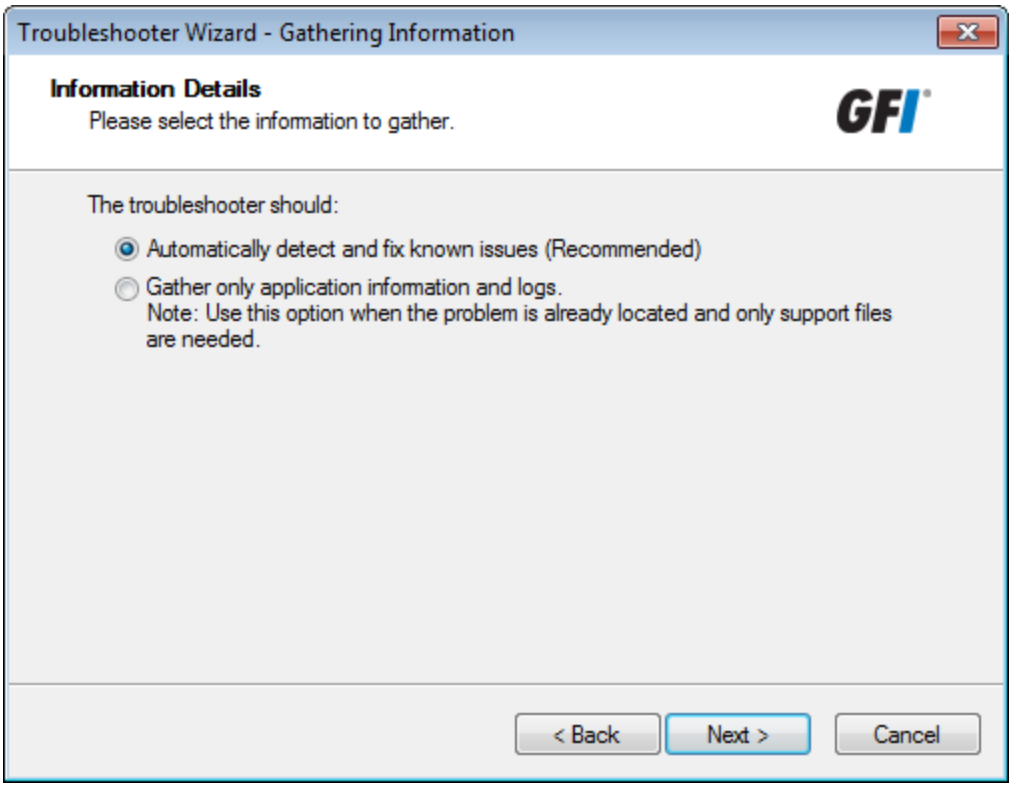
5.2 Utilización del asistente para el solucionador de problemas

El asistente para el solucionador de problemas de GFI LanGuard es una herramienta diseñada para brindarle asistencia cuando encuentre problemas técnicos relacionados con GFI LanGuard. A través de este asistente, puede detectar y solucionar de forma automática problemas comunes y recopilar información y registros para enviarlos a nuestro equipo de asistencia técnica.

Para utilizar el asistente para el solucionador de problemas:

1. Inicie el asistente de solución de problemas en **Inicio > Programas > GFI LanGuard 2015 > GFI LanGuard 2015 Troubleshooter** (solucionador de problemas).

2. Haga clic en **Next** en la página de introducción.


Troubleshooter Wizard - Gathering Information
Information Details
Please select the information to gather.
GFI
The troubleshooter should:
Automatically detect and fix known issues (Recommended)
Gather only application information and logs.
Note: Use this option when the problem is already located and only support files are needed.
< Back
Next >
Cancel

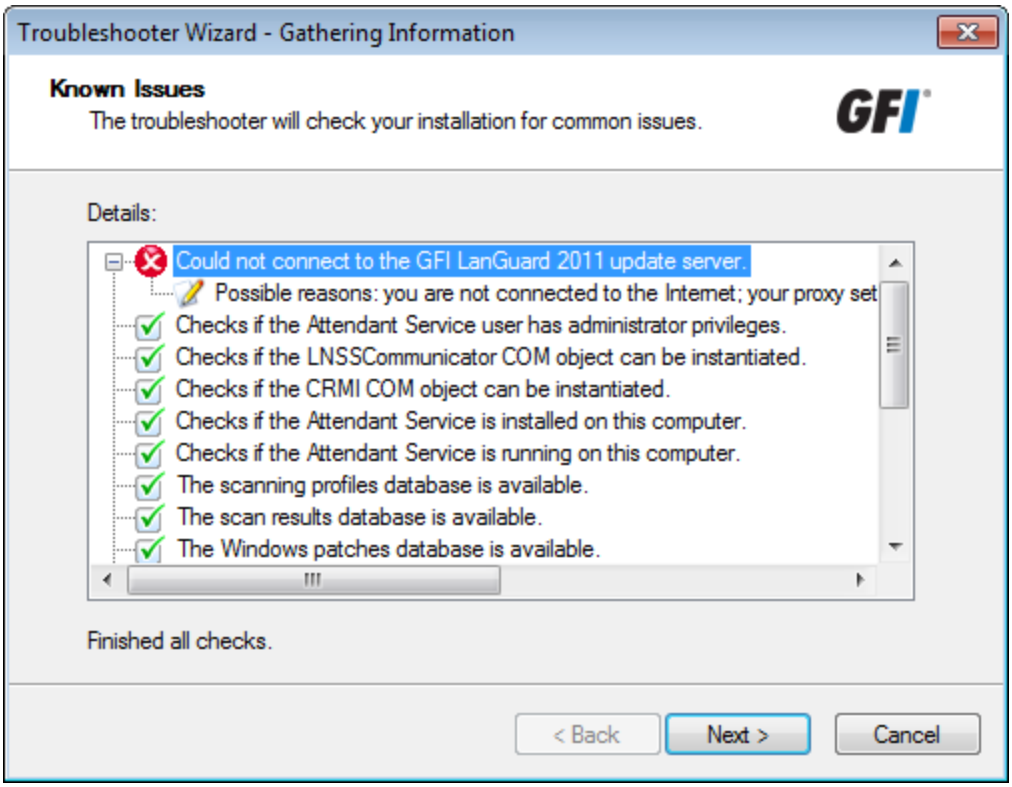
Captura de pantalla 24: Asistente para el solucionador de problemas: detalles de información

3. En la página Information Details seleccione una de las siguientes opciones descritas a continuación:

Tabla 19: Opciones de recopilación de información

Opción	Descripción
Automatically detect and fix known issues (Recommended)	Permite configurar GFI LanGuard para que detecte y solucione problemas de forma automática.
Gather only application information and logs	Permite recopilar registros para enviarlos al servicio de asistencia de GFI.

4. Haga clic en **Next** para continuar.


Troubleshooter Wizard - Gathering Information
Known Issues
The troubleshooter will check your installation for common issues.
GFI
Details:
Could not connect to the GFI LanGuard 2011 update server.
Possible reasons: you are not connected to the Internet; your proxy set
Checks if the Attendant Service user has administrator privileges.
Checks if the LNSSCommunicator COM object can be instantiated.
Checks if the CRMI COM object can be instantiated.
Checks if the Attendant Service is installed on this computer.
Checks if the Attendant Service is running on this computer.
The scanning profiles database is available.
The scan results database is available.
The Windows patches database is available.
Finished all checks.
< Back
Next >
Cancel

Captura de pantalla 25: Asistente para el solucionador de problemas: recopilación de información sobre problemas conocidos

5. El asistente para el solucionador de problemas recuperará toda la información requerida para resolver problemas comunes. Haga clic en **Next** para continuar.

6. El solucionador de problemas solucionará cualquier problema conocido que encuentre. Seleccione **Yes** si su problema se ha resuelto o **No** si esto ha sucedido para buscar información en la Knowledge Base de GFI Knowledge.

5.3 GFI SkyNet

GFI mantiene un exhaustivo repositorio de su base de conocimientos, que incluye respuestas a los problemas más habituales. GFI SkyNet tiene siempre la lista más actualizada de preguntas y revisiones de asistencia técnica. Si la información de esta guía no soluciona sus problemas, consulte GFI SkyNet visitando: http://kb.gfi.com/.

5.4 Foro web

La asistencia técnica técnica de usuario a usuario está disponible a través del foro de la red de GFI. Acceda al foro web visitando: http://forums.gfi.com

5.5 Solicitud de asistencia técnica

Si ninguno de los recursos especificados anteriormente le permite solucionar los problemas, póngase en contacto con el equipo de asistencia técnica de GFI completando un formulario de solicitud de asistencia técnica en línea, o bien por vía telefónica.

- **En línea**: complete el formulario de solicitud de asistencia técnica y siga las instrucciones de esta página con atención para enviar su solicitud de asistencia técnica en: http://-support.gfi.com/supportrequestform.asp.
- **Por teléfono**: para obtener el número de teléfono de asistencia técnica correcto de su área, visite: http://www.gfi.com/company/contact.htm.

Nota

Antes de ponerse en contacto con el servicio de asistencia técnica, tenga su ID de cliente a mano. Su ID de cliente es el número de cuenta en línea que se le asigna cuando registra sus claves de licencia en el área de clientes de GFI en: http://customers.gfi.com.

Enviaremos una respuesta a su solicitud en 24 horas o antes, según su zona horaria.

Documentación

Si este manual no cumple sus expectativas o si cree que esta documentación se puede mejorar, indíquenoslo enviando un correo electrónico a: documentation@gfi.com.

6 Glosario

A

Access™

Sistema de administración de bases de datos relacionales de escritorio de Microsoft® incluido en el paquete de Microsoft® Office. Access™ normalmente se utiliza para bases de datos pequeñas.

Active Directory™ (AD)

Tecnología que proporciona diversos servicios de red, entre los que se incluyen los servicios de directorio similares a LDAP.

Administración de revisiones automática

Tecnología de GFI LanGuard que descarga de forma automática actualizaciones de Microsoft® y las implementa en la red.

Agente de revisión

Servicio de fondo que administra la implementación de revisiones, Service Pack y actualizaciones de software en equipos de destino.

Antispyware

Contramedida de software que detecta spyware que se ha instalado en un equipo sin que el usuario lo sepa.

Antivirus

Contramedida de software que detecta malware que se ha instalado en un equipo sin que el usuario lo sepa.

Archivos de procesamiento por lotes

Archivos de texto que contienen una recopilación de instrucciones que un sistema operativo o una aplicación deben seguir

B

Base de datos de Microsoft® Access™

Sistema de administración de bases de datos relacionales de escritorio de Microsoft® incluido en el paquete de Microsoft® Office. Microsoft® Access™ normalmente se utiliza para bases de datos pequeñas.

Bluetooth

Protocolo inalámbrico abierto de comunicación e interfaz que permite el intercambio de datos entre dispositivos.

Bus serie universal (USB)

Estándar de bus serie ampliamente utilizado para conectar dispositivos a un equipo host.

C

Corrección automática

Tecnología de GFI LanGuard que descarga e implementa de forma automática revisiones faltantes. Si una aplicación se encuentra en la lista negra en GFI LanGuard, la corrección automática la desinstalará del equipo de destino durante las operaciones programadas.

D

deploycmd.exe

Herramienta de línea de comandos de GFI LanGuard que se utiliza para implementar revisiones de Microsoft® y software de terceros en equipos de destino.

Depurador de scripts

Módulo de GFI LanGuard que le permite escribir y depurar scripts personalizados utilizando un lenguaje compatible con VBScript.

Descarga automática

Tecnología de GFI LanGuard que descarga de forma automática revisiones y Service Pack faltantes en los 38 idiomas.

Desinstalación automática de aplicaciones

Acción que permite la desinstalación automática de aplicaciones compatibles con la desinstalación silenciosa de GFI LanGuard.

DMZ

Sección de una red que no es parte de la red interna y que no forma parte de Internet de manera directa. Su objetivo es generalmente actuar como puerta de enlace entre las redes internas e Internet.

DNS

Base de datos que utilizan las redes TCP e IP, que permite la conversión de nombres de host en números IP y el suministro de otra información relacionada con dominios.

F

FTP

Protocolo que se utiliza para transferir archivos entre equipos de redes.

G

GFI EndPointSecurity

Solución de seguridad desarrollada por GFI que permite a las organizaciones conservar la integridad de datos evitando el acceso no autorizado y las transferencias de dispositivos extraíbles.

GPO

Sistema de administración y configuración centralizado de Active Directory que controla lo que los usuarios pueden y no pueden hacer en una red informática.

H

Herramienta de auditoria de SNMP

Herramienta que informa cadenas de comunidad de SNMP vulnerables mediante un ataque por diccionario con los valores almacenados en su archivo de diccionario predeterminado.

Herramienta de auditoría de SQL Server

Herramienta que se utiliza para probar la vulnerabilidad de la contraseña de la cuenta de "sa" (es decir, administrador raíz) y de cualquier otra cuenta de usuarios de SQL configurada en SQL Server.

Herramienta DNS Lookup

Utilidad que convierte nombres de dominio en la dirección IP correspondiente y recupera información en particular del dominio de destino

Herramienta Enumerate Computers

Utilidad que identifica dominios y grupos de trabajo en una red.

Herramienta SNMP Walk

Herramienta que se utiliza para sondear sus nodos de red y recuperar información de SNMP.

Herramienta Traceroute

Herramienta que se utiliza para idenfiticar la ruta de acceso que GFI LanGuard ha empleado para alcanzar un equipo de destino.

Herramienta Whois

Herramienta que le permite buscar información en un dominio o una dirección IP en particular.

Herramientas para enumerar equipos

Herramientas que le permiten recuperar usuarios e información sobre usuarios de su dominio o grupo de trabajo.

I

impex.exe

Herramienta de línea de comandos que se utiliza para importar y exportar perfiles y vulnerabilidades de GFI LanGuard.

Información de boletín.

Contiene una recopilación de información sobre una revisión o actualización de Microsoft®. Se utiliza en GFI LanGuard para proporcionar más información en una revisión o actualización instaladas. La información incluye ID de boletín, título, descripción, URL y tamaño de archivo.

Interfaz de puerta de enlace común (CGI)

Script de comunicación utilizado por servidores web para transferir datos a un explorador de Internet de clientes.

Internet Information Services (IIS)

Conjunto de servicios basados en Internet, creados por Microsoft® Corporation para servidores de Internet.

L

Lenguaje abierto de vulnerabilidad y evaluación (OVAL)

Estándar que promueve contenido de seguridad abierto y públicamente disponible, y estandariza la transferencia de esta información en todo el espectro de herramientas y servicios de seguridad.

Lenguaje de marcado extensible (XML)

Estándar de texto abierto que se utiliza para definir formatos de datos. GFI LanGuard utiliza este estándar para importar o exportar resultados de examen guardados y configuraciones.

Linux

Sistema operativo de código abierto que forma parte de la familia de sistemas operativos Unix.

Lista blanca

Lista de nombres de dispositivos USB o de red no considerados peligrosos. Cuando el nombre de un dispositivo USB o de red contiene una entrada que se halla en la lista blanca durante el examen de una red, GFI LanGuard ignora el dispositivo y lo considera como una fuente segura.

Lista negra

Lista de dispositivos USB o de red considerados peligrosos. Cuando el nombre de un dispositivo USB o de red contiene una entrada que se halla en la lista negra durante el examen de una red, GFI LanGuard presenta el dispositivo como una amenaza de seguridad (vulnerabilidad de seguridad alta).

lnsscmd.exe

Herramienta de línea de comandos de GFI LanGuard que permite la ejecución de comprobaciones de vulnerabilidades en destinos de red.

Localhost

En redes, el localhost es el equipo que se utiliza en el momento. Se puede consultar el localhost utilizando la dirección IP reservada 127.0.0.1. En este manual, el localhost es el equipo en el que GFI LanGuard está instalado.

Localizador uniforme de recursos (URL)

El Localizador uniforme de recursos es la dirección de una página web de la World Wide Web.

M

Malware

Compuesto por “malintencionado” y “software”, malware es un término general que se utiliza para citar todo software desarrollado para perjudicar y dañar el sistema de un equipo. Los virus, gusanos y troyanos son todos tipos de malware.

Microsoft® IIS

Conjunto de servicios basados en Internet, creados por Microsoft® Corporation para servidores de Internet.

Microsoft® WSUS

Acrónimo que representa “Microsoft® Windows Server Update Services”. Este servicio permite a los administradores gestionar la distribución de actualizaciones de Microsoft® a equipos de red.

Módulo SSH

Módulo que se utiliza para determinar el resultado de las comprobaciones de vulnerabilidades a través de los datos (texto) de la consola producidos por un script ejecutado. Esto significa que puede crear comprobaciones de vulnerabilidades de Linux o UNIX personalizadas utilizando cualquier método de scripting compatible con los SO Linux o UNIX de destino, que envíe resultados a la consola en texto.

N

NETBIOS

Acrónimo que representa “sistema básico de entrada y salida de red”. Este sistema proporciona servicios para que las aplicaciones de diferentes equipos de una red se puedan comunicar entre sí.

Netscape

Explorador web desarrollado originalmente por Netscape Communications Corporation.

O

Objeto de directiva de grupo (GPO)

Sistema de administración y configuración centralizado de Active Directory que controla lo que los usuarios pueden y no pueden hacer en una red informática.

OVAL

Estándar que promueve contenido de seguridad abierto y públicamente disponible, y estandariza la transferencia de esta información en todo el espectro de herramientas y servicios de seguridad.

P

Panel

Representación gráfica que indica el estado de varias operaciones que podrían estar actualmente activas, o que están programadas.

Perfiles de examen

Recopilación de comprobaciones de vulnerabilidades que determinan qué vulnerabilidades se identifican y qué información se recuperará de los destinos examinados.

Pings de ICMP

El protocolo de mensajes de control de Internet (ICMP) es uno de los protocolos principales del conjunto de protocolos de Internet. Lo utilizan los sistemas operativos de equipos en red para enviar mensajes de error que indican, por ejemplo, que un servicio solicitado no se encuentra disponible o que un host o enrutador no se han podido alcanzar. El ICMP también se puede utilizar para la retransmisión de mensajes de solicitudes.

Programa de puerta trasera

Método alternativo utilizado para acceder a un equipo o a datos de un equipo a través de una red.

Protocolo de escritorio remoto

Protocolo desarrollado por Microsoft® para permitir que los clientes se conecten con la interfaz de usuario de un equipo remoto.

Protocolo de mensajes de control de Internet (ICMP)

El protocolo de mensajes de control de Internet (ICMP) es uno de los protocolos principales del conjunto de protocolos de Internet. Lo utilizan los sistemas operativos de equipos en red para enviar mensajes de error que indican, por ejemplo, que un servicio solicitado no se encuentra disponible o que un host o enrutador no se han podido alcanzar. El ICMP también se puede utilizar para la retransmisión de mensajes de solicitudes.

Protocolo de transferencia de archivos

Protocolo que se utiliza para transferir archivos entre equipos de redes.

Protocolo simple de administración de redes (SNMP)

El protocolo simple de administración de redes es una tecnología que se utiliza para controlar dispositivos de red como enrutadores, concentradores y connmutadores.

Puertos TCP

Acrónimo que representa “Protocolo de control de transmisión”. Este protocolo está desarrollado para permitir que las aplicaciones transmitan y reciban datos a través de Internet utilizando puertos de equipos conocidos.

Puertos UDP

Acrónimo que representa “Protocolo de datagramas de usuario”; se utiliza para transferir datos de UDP entre dispositivos. En este protocolo, los paquetes recibidos no se reconocen.

S

SANS

Acrónimo que significa “Organización investigadora para la administración de sistemas, las redes y la seguridad”. Instituto que comparte soluciones relacionadas con alertas de sistema y seguridad.

Scripting Python

Lenguaje de scripting de programación de equipos de alto nivel.

Service Pack de Microsoft® Windows

Recopilación de actualizaciones y correcciones proporcionadas por Microsoft® para mejorar una aplicación o un sistema operativo.

Servicios de terminal

Servicios que permite la conexión con un equipo de destino y la administración de sus aplicaciones instaladas y datos almacenados.

Servidor de correo

Servidor que administra y almacena correos electrónicos clientes.

Servidor web

Servidor que proporicona páginas web a exploradores clientes utilizando el protocolo HTTP.

Servidor web Apache

Projecto de servidor HTTP de código abierto desarrollado y mantenido por la Apache Software Foundation.

Sistema de nombres de dominio

Base de datos que utilizan las redes TCP e IP, que permite la conversión de nombres de host en números IP y el suministro de otra información relacionada con dominios.

SNMP

Acrónimo que representa “Protocolo simple de administración de redes”, una tecnología que se utiliza para controlar dispositivos de red como enrutadores, concentradores y conmutadores.

Spyware

Forma de malware pensada para recopilar información de un equipo sin notificar al usuario.

SQL Server®

Sistema de administración de bases de datos relacionales de Microsoft®. Funcionalidad adicional incluida de Microsoft® para SQL Server® (control de transacciones, manipulación de excepciones y seguridad), a fin de que Microsoft SQL Server® pueda admitir organizaciones grandes.

T

Troyanos

Forma de malware que contiene una aplicación oculta que dañará un equipo.

U

URL

El Localizador uniforme de recursos es la dirección de una página web de la World Wide Web.

V

VBScript

Un lenguaje de scripting de Visual Basic es un lenguaje de programación de alto nivel desarrollado por Microsoft®.

Virus

Forma de malware que infecta un equipo. El propósito de este virus es perjudicar un equipo dañando archivos y aplicaciones. Un virus es un programa de duplicación automática y se puede copiar a sí mismo en todo el sistema del equipo.

Vulnerabilidades y exposiciones comunes (CVE)

Lista de nombres estandarizados para vulnerabilidades y otras exposiciones de seguridad de la información. El propósito de CVE es estandarizar los nombres para todas las vulnerabilidades y exposiciones de serguridad de conocimiento público.

W

Wi-Fi/LAN inalámbrica

Tecnología que se utiliza comúnmente en redes de área local. Los nodos de red utilizan datos transmitidos mediante ondas de radio en lugar de cables para comunicarse entre sí.

X

XML

Estándar de texto abierto que se utiliza para definir formatos de datos. GFI LanGuard utiliza este estándar para importar o exportar resultados de examen guardados y configuraciones.

Z

Zona desmilitarizada (DMZ)

Sección de una red que no es parte de la red interna y que no forma parte de Internet de manera directa. Su objetivo es generalmente actuar como puerta de enlace entre las redes internas e Internet.

7 Índice

A

Actualización 17

Actualizaciones de seguridad 36

Administración de revisiones 13

Agente 11, 34

Agentes de retransmisión 6, 16

Auditoría 4, 16

B

Búsqueda de texto completo 28

C

Componentes 6, 12

Consola de administración 6

D

Descarga automática 4

E

Equipo 30

Evaluación de vulnerabilidades 13

H

Hardware 33, 37, 45

Hardware Audit 13

I

Importar 17

Instalación 7, 34

N

NetBIOS 16

Notificaciones 4

O

OVAL 4

P

Panel 23

Puertos 11, 37

Puertos TCP abiertos 37

Puertos UDP abiertos 37

R

Registro remoto 15

Remediation Center 32, 39

S

Service Pack y paquetes acumulativos de actualizaciones faltantes 36

Service Pack y paquetes acumulativos de actualizaciones instalados 36

Servidor 6, 11

SMB 5, 17, 48

SNMP 16

Software 33, 37, 43

Software Audit 13

SQL 14, 47

SSH 15

U

Uso compartido de archivos e impresoras 15

Usuarios de la sesión actual 28, 37

V

Vulnerabilidades 35

W

WMI 5, 15

EE.UU., CANADÁ, AMÉRICA CENTRAL Y AMÉRICA DEL SUR

4309 Emperor Blvd, Suite 400, Durham, NC 27703, USA

Teléfono: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

RU Y REPÚBLICA DE IRLANDA

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, UK

Teléfono: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPA, ORIENTE MEDIO Y ÁFRICA

GFI House, Territorials Street, Mriehel BKR 3000, Malta

Teléfono: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA Y NUEVA ZELANDA

83 King William Road, Unley 5061, South Australia

Teléfono: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com